

POINT COUNTING IN FAMILIES OF HYPERELLIPTIC CURVES IN CHARACTERISTIC 2

HENDRIK HUBRECHTS

Abstract

Let \bar{E}_Γ be a family of hyperelliptic curves over $\mathbb{F}_2^{\text{alg cl}}$ with general Weierstrass equation given over a very small field \mathbb{F} . We describe in this paper an algorithm for computing the zeta function of \bar{E}_γ , with γ in a degree n extension field of \mathbb{F} , which has as time complexity $\tilde{O}(n^3)$ bit operations and memory requirements $O(n^2)$ bits. With a slightly different algorithm we can get time $O(n^{2.667})$ and memory $O(n^{2.5})$, and the computation for n curves of the family can be done in time $\tilde{O}(n^{3.376})$. All of these algorithms are polynomial-time in the genus.

1. Introduction and results

The problem of counting the number of rational points on curves over finite fields has received much attention during the last decade. The main reason for this in fact renewed interest is the proposal of several applications such as cryptographic protocols which use such curves. For most of these applications it is very important to know the cardinality of the curve, in [4] and [3] an overview of some of these applications can be found. Working with finite fields of characteristic 2 is particularly interesting due to the fact that computers can work very efficiently with them.

In the course of the recent research a lot of algorithms have been proposed, most of them focused on elliptic curves. We will give an overview of some of these results, in particular of those most related to the work that we present in this paper, namely hyperelliptic curves in characteristic 2. When discussing these algorithms, and also in the rest of the paper, we will give all running times and memory requirements using either number of bit operations or bit space. The notation \tilde{O} is defined in [23, Definition 25.8] and is essentially a O -notation that ignores logarithmic factors. We assume that the curves below are defined over the finite field \mathbb{F}_q where $q = p^n$ for some prime number p .

A first general algorithm for elliptic curves was ℓ -adic in nature, and due to Schoof. Here ℓ is a prime different from p . Improvements of Elkies and Atkin resulted in the well-known SEA algorithm [8], that works in time $\tilde{O}((\log q)^4)$ and has $\tilde{O}((\log q)^2)$ as space complexity. For higher genus these ℓ -adic methods turned out not to be very useful, and only the genus 2 case has been developed in practice [9].

For small characteristic, p -adic methods seem to be much more efficient, and as a consequence many algorithms, especially for higher genus, are of this kind. A first algorithm was given by Satoh for elliptic curves [18], and after some development by several authors this culminated in an algorithm with running time $\tilde{O}(n^2)$ by Harley (unpublished, all details

The author is Research Assistant of the Research Foundation - Flanders (F.W.O. - Vlaanderen)

2000 Mathematics Subject Classification 11G20, 11Y99, 12H25, 14F30, 14G50, 14Q05

© ????, Hendrik Hubrechts

can however be found in [21, Section 3.10]). We will come back to some ideas of this algorithm in Section 5.1. Another approach uses the arithmetic geometric mean (AGM) and was proposed by Mestre. It worked originally in time $\tilde{O}(n^3)$, but Lercier and Lubicz improved this to $\tilde{O}(n^2)$ for fields where a Gaussian normal basis is available. The AGM algorithm works not only for elliptic curves, but the dependency on the genus is exponential.

The first algorithm for general hyperelliptic curves that works polynomially in the genus g was given by Kedlaya in [13], its time complexity is $\tilde{O}(g^4 n^3)$ and it uses $O(g^3 n^3)$ space. Kedlaya uses a ‘rigid analytic lift’ to characteristic zero of the curve, and needs an explicit equation of the curve in order to construct a Frobenius map on the resulting Monsky-Washnitzer cohomology. Due to the more complicated structure of curves in characteristic 2, Kedlaya’s algorithm did not cover this situation, and it was subsequently handled in Denef and Vercauteren’s paper [7].

A totally different approach to point counting was proposed by Lauder [15] and Tsuzuki [20], first developed to tackle higher dimensional varieties. It consists of embedding the variety in a family in such a way that some fiber of the family gives rise to an ‘easy case’, and the other fibers can then be treated in an efficient way. This turns out to reduce highly the dependency on the dimension. However, Denef and Lauder realised that this might also be useful for hyperelliptic curves in odd characteristic, and this suggestion from [16] was worked out by the author in a previous paper [12]. It essentially consists of combining Kedlaya’s method with a one dimensional deformation. The main result is an algorithm that computes the zeta function of curves within certain families in time $\tilde{O}(g^{6.376} n^3)$ and space $\tilde{O}(g^5 n^2)$, although also time $\tilde{O}(g^{6.376} n^{2.667})$ turned out to be possible. In the present paper we extend these results to the characteristic 2 case by reconciling Denef and Vercauteren’s work with such a deformation.

In [10] Gerkmann also considered a deformation approach for elliptic curves in odd characteristic and at the end of the paper he handles the family of elliptic curves with equation $Y^2 + XY = X^3 + \gamma X$ for $\gamma \in \mathbb{F}_2^{\text{alg}}$. The particular form of this equation makes this relatively easy, but for higher genus the equations are much more involved. As a consequence the theory is technically rather different from the odd characteristic case, although the ‘big picture’ has a similar *esprit*.

We will now present the results proven in this paper. Let \mathbb{F}_q be a finite field with $q = 2^a$ elements, $\bar{\gamma} \in \mathbb{F}_{q^n}$ for some integer n , and $g \geq 1$ an integer. Suppose $\bar{f}, \bar{h} \in \mathbb{F}_q[X, \Gamma]$ are in the form described in Section 2.1, which implies in particular that we get a hyperelliptic curve of genus g over \mathbb{F}_{q^n} given by the equation

$$\bar{E}_{\bar{\gamma}} : Y^2 + \bar{h}(X, \bar{\gamma})Y = \bar{f}(X, \bar{\gamma}).$$

Define $\kappa := \max\{\deg_{\Gamma} f, \deg_{\Gamma} h^2\}$. As is mentioned in [7], in this matter we have an ‘average case’ and a ‘worst case’. This means that almost all curves belong to the first case, and some unlucky ones do not. The main result is the following theorem, proven in Section 5.

THEOREM 1. *We can compute deterministically the zeta function of (the projective completion of) $\bar{E}_{\bar{\gamma}}$ using $\tilde{O}(g^{6.376} a^3 \kappa^2 n^2 + g^{3.376} a^3 n^3)$ bit operations and $\tilde{O}(g^4 a^3 \kappa n^2)$ bits of memory ‘on average’. For the ‘worst case’ situation one factor g has to be added to the terms with n^2 in them.*

We note that the algorithm allows us also to compute the matrix of the 2nd power Frobenius in time quasi-quadratic in n , whereas Kedlaya’s algorithm requires cubic time for this.

It is only during the computation of the matrix of the q^{th} power Frobenius that the estimate $\tilde{O}(g^{3.376}a^3n^3)$ of Theorem 1 appears. This step can be done faster by using advanced polynomial composition techniques, at the cost of an increase in memory usage. The result is the following.

THEOREM 2. *There exists a deterministic algorithm that computes the zeta function of $\bar{E}_{\bar{\gamma}}$ in $\tilde{O}(g^{6.376}a^3\kappa^2n^2 + g^{3.376}a^3n^{2.667})$ bit operations ‘on average’. It requires $\tilde{O}(g^4a^3\kappa n^2 + g^3a^2n^{2.5})$ bits of memory. In the ‘worst case’ again one factor g has to be added to both first terms.*

It is worth noting that with ω the exponent for matrix multiplication, currently known to satisfy $\omega < 2.376$ (see [5]), the above time complexity is in fact $\tilde{O}(g^{4+\omega}a^3\kappa^2n^2 + g^{1+\omega}a^3n^{\min(2.667, (3+\omega)/2)})$.

Theorem 2 together with the following theorem is proven in Section 6. In this theorem we did not pay attention to the dependency on parameters different from n .

THEOREM 3. *Given n parameters $\bar{\gamma}_1, \dots, \bar{\gamma}_n \in \mathbb{F}_{q^n}$, it is possible to find the zeta functions of all $\bar{E}_{\bar{\gamma}_i}$ with $\tilde{O}(n^{3.376})$ as time and $O(n^3)$ as space requirements.*

The bottom line of this algorithm is that in order to find a curve with some special size by trying a lot of curves, we can count on $\tilde{O}(n^{2.376})$ as the time needed for one curve. Again we have in fact $\tilde{O}(n^{1+\omega})$ as time complexity in Theorem 3. In Section 6 we explain also shortly an $\tilde{O}(n^2)$ algorithm for a special situation where a Gaussian normal basis is present. We have to note however that the use of this last result is very limited.

Theorems 1 and 2 can be compared with the algorithms mentioned earlier: Denef and Vercauteren require ‘on average’ $\tilde{O}(g^4n^3)$ bit operations and $O(g^3n^3)$ bits of memory, and the algorithm of Lercier and Lubicz has time complexity $\tilde{O}(2^g n^2)$.

This paper is organised as follows. In Section 2 we provide the theory behind the algorithm, in it is explained the required special form of \bar{f} and \bar{h} , to which we referred earlier. The algorithm uses a ‘matrix differential equation’ with 2-adic matrices as coefficients, and in Section 3 we have gathered some necessary results about these kinds of objects. More precisely, some trick is explained that allows us to compute the matrix of the connection and a particularly useful form of the differential equation, the convergence properties of Frobenius are investigated and an important result about error propagation is established. The next section gives the algorithm and proves its correctness, and Section 5 estimates the complexity, thereby proving Theorem 1. Finally the last section explains the improvements noted above, in particular Theorems 2 and 3.

The author wishes to thank very much Jan Denef for his thorough proofreading of the paper, the referee for the helpful comments and Frederik Vercauteren for drawing attention to the relevance of results as those of Section 6.3.

2. Analytic theory

In this section we will develop an analytic theory which combines the results from [7] with a deformation. Before we start let us define some notation used throughout the rest of the paper. Let a be a strictly positive integer and denote by \mathbb{F}_q the finite field with $q := 2^a$ elements. Let \mathbb{Q}_2 be the completion of \mathbb{Q} according to the 2-adic valuation and \mathbb{Q}_q the unique degree a unramified extension of \mathbb{Q}_2 . Denote with \mathbb{C}_2 the completion of an algebraic

closure of \mathbb{Q}_2 . The notation ord or ord_2 is used for the valuation on \mathbb{C}_2 , normalised to $\text{ord}_2(2) = 1$. The ring of integers of \mathbb{Q}_q is written as \mathbb{Z}_q and the lift of the 2nd power Frobenius automorphism on \mathbb{F}_q is given by $\sigma : \mathbb{Q}_q \rightarrow \mathbb{Q}_q$. We extend σ by letting it act as squaring on each appearing variable. If k is a field, then we mean by $k^{\text{alg cl}}$ an algebraic closure of k . The derivative of a function $\alpha = \alpha(X, \Gamma)$ with respect to X will be denoted by α' , and on the other hand $\frac{\partial \alpha}{\partial \Gamma}$ is written as $\dot{\alpha}$.

2.1. Introducing the deformation.

Suppose we are given an equation $Y^2 + \bar{h}(X) \cdot Y = \bar{f}(X)$ over \mathbb{F}_q which defines a hyperelliptic curve of genus g . As pointed out in [7] it is always possible to find in an efficient way an isomorphic curve over \mathbb{F}_q given by $Y^2 + \bar{h}(X) \cdot Y = \bar{f}(X)$ subject to the following conditions. The degree of the monic polynomial \bar{f} is $2g + 1$ and \bar{h} is nonzero of degree at most g . If we factor \bar{h} in its monic irreducible factors over \mathbb{F}_q , $\bar{h}(X) = \bar{c} \prod_{i=1}^t \bar{h}_i^{r_i}(X)$ with all \bar{h}_i irreducible and pairwise distinct, $r_i \neq 0$ and $\bar{c} \in \mathbb{F}_q^\times$, define then $\bar{H}(X) := \prod_{i=1}^t \bar{h}_i(X)$, the product of the irreducible factors of \bar{h} . We require now that $\bar{f} = \bar{H} \cdot \bar{Q}_{\bar{f}}$ where \bar{H} and $\bar{Q}_{\bar{f}}$ are relatively prime. Define $\bar{D} := \max r_i$ so that \bar{h} is a divisor of $\bar{H}^{\bar{D}}$, and let $\bar{Q}_{\bar{h}}$ be such that $\bar{h} \cdot \bar{Q}_{\bar{h}} = \bar{H}^{\bar{D}}$.

We will now introduce the deformation parameter Γ . Choose $t \in \mathbb{Z}_{\geq 0}$, let $d_1, \dots, d_t, r_1, \dots, r_t$ be positive nonzero integers such that $d_1 r_1 + \dots + d_t r_t \leq g$, choose $c(\Gamma) \in \mathbb{Z}_q[\Gamma]$ and let $\tilde{D} := \max r_i$. We refer to the end of this subsection for the special case where $t = 0$. Choose polynomials h_1, \dots, h_t, Q_f in $\mathbb{Z}_q[X, \Gamma]$, monic in X , with $\deg_X h_i = d_i$ for all i , and $\deg_X Q_f = 2g + 1 - \sum_i d_i$. Define $H := \prod_i h_i$, $h := c \prod_i h_i^{r_i}$, $f := H Q_f$ and $Q_h := c H^{\tilde{D}} / h$. Let $r(\Gamma)$ be equal to $c(\Gamma)$ multiplied with a certain resultant:

$$r(\Gamma) := c(\Gamma) \cdot \text{Res}_X \left(H(X, \Gamma), Q_f(X, \Gamma) \cdot \frac{\partial H(X, \Gamma)}{\partial X} \right) = c \cdot \text{Res}_X(H, Q_f H').$$

Then we require $r(\Gamma)$ to be a polynomial for which $r(0)$ does not reduce to zero modulo 2, or equivalently $\Gamma = 0$ gives a hyperelliptic curve modulo 2 in Weierstrass form as follows from Lemma 4 below. The polynomial $r(\Gamma)$ determines for which parameters the result is a hyperelliptic curve of genus g , therefore we define the following subset of the set $\text{Teich}(\mathbb{F}_2^{\text{alg cl}})$ of Teichmüller lifts in \mathbb{C}_2 of $\mathbb{F}_2^{\text{alg cl}}$ (for ease of notation we say that $0 \in \mathbb{C}_2$ is also a Teichmüller lift):

$$\mathbb{S} := \left\{ \gamma \in \text{Teich}(\mathbb{F}_2^{\text{alg cl}}) \mid r(\gamma) \not\equiv 0 \pmod{2} \right\}.$$

The requirement $r(0) \not\equiv 0 \pmod{2}$ implies that \mathbb{S} is an infinite set that contains 0.

We denote with $\bar{\cdot}$ the projection modulo 2 for all these polynomials, hence $\bar{h}_i(X, \Gamma)$ is from now on the projection of $h_i(X, \Gamma)$ and so on.

LEMMA 4. *For $\bar{\gamma} \in \mathbb{F}_2^{\text{alg cl}}$ the projected equation $Y^2 + \bar{h}(X, \bar{\gamma}) \cdot Y = \bar{f}(X, \bar{\gamma})$ defines a hyperelliptic curve $\bar{E}_{\bar{\gamma}}$ of genus g if and only if $\text{Teich}(\bar{\gamma}) \in \mathbb{S}$.*

Proof. It is enough to show for a Teichmüller lift γ that $\bar{E}_{\bar{\gamma}}$ has no affine singularities if and only if $\gamma \in \mathbb{S}$. When $\bar{c}(\bar{\gamma}) = 0$, it is clear that the curve has an affine singularity, so we suppose $\bar{c}(\bar{\gamma}) \neq 0$. Computing the system of partial derivatives yields immediately that the existence of an affine singularity (\bar{x}, \bar{y}) implies that $\bar{H}(\bar{x}) = \bar{h}(\bar{x}) = \bar{f}(\bar{x}) = \bar{y} = 0$ and $\bar{f}'(\bar{x}) = 0$, and vice versa: these equalities give an affine singularity. As $\bar{f}' = \bar{Q}'_{\bar{f}} \bar{H} + \bar{Q}_{\bar{f}} \bar{H}'$

we conclude that $\bar{E}_{\bar{\gamma}}$ has no affine singularities if and only if the system $\bar{H} = \bar{Q}_f \bar{H}' = 0$ has no solutions, which in turn is equivalent to $\text{Res}_X(\bar{H}, \bar{Q}_f \bar{H}') \neq 0$. \square

The condition on the resultant guarantees that $\bar{H}(X, \bar{\gamma})$ and $\bar{Q}_f(X, \bar{\gamma})$ are relatively prime for every $\gamma \in \mathbb{S}$ and that $\bar{H}(X, \bar{\gamma})$ has no double roots. Due to the careful construction of H and h as products of the same factors, we find that $h|cH^{\bar{D}}$ and $\bar{h}|\bar{c}\bar{H}^{\bar{D}}$, hence the equation $Y^2 + \bar{h}(X, \bar{\gamma})Y = \bar{f}(X, \bar{\gamma})$ has the special form as explained in the first paragraph of this section (possibly with a bigger t , if some $\bar{h}_i(X, \bar{\gamma})$ is not irreducible over $\mathbb{F}_q(\bar{\gamma})$).

The constructions above fail when $t = 0$, in which case $\bar{c}(\bar{\gamma}) \neq 0$ is equivalent to $\bar{E}_{\bar{\gamma}}$ being hyperelliptic. In this situation we put $r(\Gamma) := c(\Gamma)$. If $\deg(r(\Gamma)) = 0$, no resultant is needed, and for example S defined below will simply be $\mathbb{Q}_q[\Gamma]^{\dagger}$. We will not always mention the simplifications needed for this special case. The convention $\bar{D} := 1$ is then best suited for the estimates further on.

As final definitions, let $\rho := \deg_{\Gamma} r(\Gamma)$, $s := \deg_X(H)$ and $\kappa := \max\{\deg_{\Gamma} f, \deg_{\Gamma} h^2\}$ as defined before, and $\eta := \deg_{\Gamma} H$. We suppose that $\kappa \geq 1$ and it is easy to see that $\rho \leq 3g\kappa$.

2.2. The overconvergent structures.

We define as in [12] the necessary overconvergent structures. For $r = \sum_{i=0}^{\rho} r_i \Gamma^i$ let ρ' be the largest index for which $\text{ord}(r_{\rho'}) = 0$, and define $\tilde{r} = \sum_{i=0}^{\rho'} r_i \Gamma^i$. Hence $\tilde{r} \equiv r \pmod{2}$ and if the leading term of r is a unit in \mathbb{Z}_q we simply have $\tilde{r} = r$. The ring S will be the equivalent of the field \mathbb{Q}_q in Denef and Vercauteren's approach.

$$S := \mathbb{Q}_q \left[\Gamma, \frac{1}{\tilde{r}(\Gamma)} \right]^{\dagger} = \left\{ \sum_{k \in \mathbb{Z}} \frac{b_k(\Gamma)}{\tilde{r}(\Gamma)^k} \mid (\forall k) b_k(\Gamma) \in \mathbb{Q}_q[\Gamma], \right. \\ \left. \deg b_k(\Gamma) < \rho' \text{ and } \liminf_k \frac{\text{ord}(b_k)}{|k|} > 0 \right\}.$$

The last inequality in this definition is equivalent to the existence of real constants $\delta > 0$ and ε such that for all k we have $\text{ord}(b_k) \geq \delta \cdot |k| + \varepsilon$. As proven in Lemma 6 of [12], the fact that $\text{ord}(\tilde{r}_{\rho'}) = 0$ implies that an expression $\sum_{i=0}^{\infty} a_i \Gamma^i + \sum_{j=1}^{\infty} \frac{b_j(\Gamma)}{\tilde{r}(\Gamma)^j}$ where $\deg b_j(\Gamma) < \rho'$, $\liminf_i \text{ord}(a_i)/|i| > 0$ and $\liminf_j \text{ord}(b_j)/|j| > 0$, represents also a general element of S . If \tilde{r} is a constant then of course $S = \mathbb{Q}_q[\Gamma]^{\dagger}$ and the parts with denominators disappear everywhere. The equality

$$\frac{1}{r} = \frac{1}{\tilde{r}} \sum_{i=0}^{\infty} \left(\frac{\tilde{r} - r}{\tilde{r}} \right)^i$$

combined with the fact that $\tilde{r} - r \equiv 0 \pmod{2}$ shows that $1/r \in S$. It is worth noting that \mathbb{S} does not change if defined using \tilde{r} instead of r , and S can be interpreted as consisting of the analytic functions defined over \mathbb{Q}_q and convergent in a disk strictly bigger than the unit disk with small disks of radius less than 1 removed around the Teichmüller lifts not in \mathbb{S} . The following important lemma is proven as Lemma 10 in [12] and gives us control over the substitution of some $\gamma \in \mathbb{S}$ in an element $s \in S$. It is easy to see that $s(\gamma)$ always converges.

LEMMA 5. Let $s(\Gamma) = \sum_{k \in \mathbb{Z}} b_k(\Gamma) / \tilde{r}(\Gamma)^k \in S$. Suppose we have for infinitely many $\gamma \in \mathbb{S}$ that $\text{ord}(s(\gamma)) \geq \alpha$ for some real number α , then also for every $k \in \mathbb{Z}$ we get $\text{ord}(b_k) \geq \alpha$.

In accordance with this lemma we will define the valuation $\text{ord}_2(s(\Gamma))$ of an element of S as the infimum (and hence minimum) of the valuations of the polynomials $b_k(\Gamma)$.

Now we can define what will be the analogue of the dagger ring A^\dagger . The last condition may look quite terrifying, but is a technical condition that implies that the sum $\sum_k s_{ik}$ is convergent and again an element of S . The notation $s^{(\cdot)}$ used below means that the conditions hold for s and s' separately.

$$T := \frac{\mathbb{Q}_q \left[\Gamma, \frac{1}{\tilde{r}(\Gamma)}, X, Y, \frac{1}{H(X, \Gamma)} \right]^\dagger}{(Y^2 + hY - f)} = \left\{ \sum_{k \in \mathbb{Z}} \frac{\sum_{i=0}^{s-1} s_{ik} X^i + \sum_{i=0}^{s-1} s'_{ik} X^i Y}{H(X, \Gamma)^k} \mid \right.$$

$$(\forall i, k) s_{ik}^{(\cdot)} \in S, (\forall i) \exists C \in \mathbb{Q}_q, \delta > 0 \text{ such that with } s_{ik}^{(\cdot)} = \sum_{j \in \mathbb{Z}} \frac{s_{ikj}^{(\cdot)}(\Gamma)}{\tilde{r}^j} \text{ where}$$

$$\left. (\forall k, j) \deg s_{ikj}^{(\cdot)}(\Gamma) < \tilde{\rho}, \text{ we have } (\forall k, j) \text{ord}(C \cdot s_{ikj}^{(\cdot)}) \geq \delta \cdot (|k| + |j|) \right\}.$$

In the case where H is a constant we have $T = \{\sum_{k \geq 0} (s_k X^k + s'_k X^k Y) \mid \text{same conditions as above}\}$, which means that in this case no denominators with respect to X occur in an element of T . We will write a general element of T as

$$\sum_{k \in \mathbb{Z}} \frac{U_k(X, \Gamma) + Y \cdot V_k(X, \Gamma)}{H^k},$$

where $U_k, V_k \in S[X]$, $\deg_X U_k$ and $\deg_X V_k$ are both at most $s-1$ and the expression satisfies the above conditions, in particular $\liminf_k \frac{\text{ord}(U_k)}{|k|} > 0$ and $\liminf_k \frac{\text{ord}(V_k)}{|k|} > 0$. It is not hard to see that T is an S -algebra.

Let $\gamma \in \mathbb{S}$ with $\tilde{\gamma} \in \mathbb{F}_{q'}$ such that $\mathbb{F}_q \subset \mathbb{F}_{q'}$ and q' is minimal. Then we can substitute γ for Γ in the above construction of T resulting in the vector space $T(\gamma) := T \otimes \mathbb{Q}_{q'} / (\Gamma - \gamma)$ over $\mathbb{Q}_{q'}$. In fact we only need the image of T under the natural map $T \rightarrow T \otimes \mathbb{Q}_{q'} / (\Gamma - \gamma)$, but the equality $\mathbb{Q}_q(\gamma) = \mathbb{Q}_{q'}$ implies that this map is surjective. We have just as in the odd characteristic case that $T(\gamma) = A^\dagger \otimes \mathbb{Q}_{q'}$ with A^\dagger as defined in Section 3.2 of [7] for the curve $Y^2 + h(X, \gamma)Y - f(X, \gamma) = 0$.

We define the derivative with respect to X on T by interpreting Y in terms of X . Using the equation in its original form and the equality $(2Y + h)^2 = 4f + h^2$ this yields

$$Y' = \frac{f' - h'Y}{2Y + h} \cdot \frac{2Y + h}{2Y + h} = \frac{f'h - 2fh' + (2f' + hh')Y}{4f + h^2}.$$

We have that $Y' \in T$ and can hence define the differential

$$d := T \rightarrow T dX : t \mapsto \frac{\partial t}{\partial X} dX.$$

Let ι be the S -linear hyperelliptic involution $X \mapsto X$ and $Y \mapsto -Y - h(X, \Gamma)$ on T , then we have the following central proposition.

PROPOSITION 6. The module $H_{MW} := \frac{TdX}{dT}$ splits into two eigenspaces under ι , namely H_{MW}^+ for eigenvalue $+1$ and H_{MW}^- for -1 . Both are free S -modules with basis respectively $\{\frac{X^i}{H}dX\}_{i=0}^{s-1}$ and $\mathcal{B} := \{b_i\}_{i=0}^{2g-1}$ with $b_i := X^i Y dX$.

If H is a constant, the first basis is empty, or equivalently H_{MW}^+ is trivial.

Proof. Let $(U + VY)H^{-k}$ be a general term of an element of T . Writing $U + VY = \tilde{U} + \tilde{V}(Y + h/2)$ and computing $\iota(Y') = -Y' - h'$ we can readily check that $\iota \circ d = d \circ \iota$, which gives the isomorphism $H_{MW} \cong H_{MW}^+ \oplus H_{MW}^-$. Here \tilde{U} gives the first part and $\tilde{V}(Y + h/2)$ the second part. The linear independence of the elements of the bases can be proven with Lemma 5. Indeed, suppose we have a linear relation $\sum_i s_i \beta_i = 0$ for basis elements β_i and $s_i \in S$ where $s_j \neq 0$. The lemma then implies the existence of some $\gamma \in \mathbb{S}$ such that $s_j(\gamma) \neq 0$, which gives a nontrivial relation $\sum_i s_i(\gamma) \beta_i(\gamma) = 0$ in the case without deformation, in contradiction with Section 3.2 of [7].

In the remainder of this proof we will use $=$ for equality in T and \equiv for equality in H_{MW} . In order to reduce a general element

$$\sum_{i \in \mathbb{Z}} U_i(X, \Gamma) dX / H^i + \sum_{j \in \mathbb{Z}} V_j(X, \Gamma) Y dX / H^j$$

of T , we consider as in Section 3.2 of [7] four cases. First, the part with $i \leq 0$ is an exact form, as integrating does not change the overconvergence property. Second, for $i > 0$ we have the following formula from [7], where $r_1(\Gamma) := \text{Res}_X(H, H')$, a divisor of $r(\Gamma)$. Write $X^k r_1(\Gamma) = A(X, \Gamma)H + B(X, \Gamma)H'$ with $A(X, \Gamma), B(X, \Gamma) \in \mathbb{Z}_q[X, \Gamma]$, then by computing the differential $d(B/H^{i-1})$ we find for $i \geq 2$

$$\frac{X^k}{H^i} dX \equiv \frac{1}{r_1} \left(\frac{A}{H^{i-1}} + \frac{B'}{(i-1)H^{i-1}} \right) dX. \quad (1)$$

Repeating this we end with $i = 1$ — which cannot be reduced further, ergo the first basis of the proposition — and an expression without denominators H which is an exact form. Next, for the part with $j \leq 0$ we can use the following congruence for $k \geq 0$

$$\left(X^k (2f' + hh') + \frac{k}{3} X^{k-1} (4f + h^2) \right) Y dX \equiv 0, \quad (2)$$

which has degree $2g + k$ in X and leading coefficient $2(2g + 1) + 4k/3 \neq 0$. We note that this congruence will be the only one needed for the algorithm.

Finally we consider the case $j > 0$. Let $h = HQ_H$, then by writing $X^k r(\Gamma) = AH + BQ_f H'$ we have

$$\frac{X^k}{H^j} Y dX \equiv \frac{1}{r} \left(\frac{A}{H^{j-1}} + \frac{B(jH'Q_H^2 - 6Q_f' - 3Q_H h') - B'(4Q_f + Q_H h)}{(6-4j)H^{j-1}} \right) Y dX + \frac{IdX}{rH}. \quad (3)$$

Here the last term $IdX/(rH)$ is an S -linear combination of the basis elements $X^i dX/H$.

Although the above formulae allow us to reduce elements of T , they do not guarantee a priori that the reduced elements and the exact differentials appearing are overconvergent. We will prove this for the case $j \leq 0$, the other cases are similar — the basic idea being that the valuations decrease by only logarithmic behaviour and deg_Γ and ‘ deg_r ’ increase at

most linearly. Let τ be an element of T of the following form:

$$\tau = \sum_{j=0}^{\infty} s_j(\Gamma) X^j Y dX.$$

If we write $s_j(\Gamma) = \sum_i s_{ij}(\Gamma) \tilde{r}(\Gamma)^i$, we may suppose — if necessary after multiplying τ with some constant — that $\text{ord}(s_{ij}) \geq \delta(j + |i|)$ for some $\delta > 0$. Applying formula (2) once to some $X^j Y dX$ in order to decrease the degree in X adds at most κ to the degree in Γ . So, if we express $X^j Y dX$ as an S -linear combination of the elements of the basis \mathcal{B} plus an exact differential,

$$X^j Y dX = \sum_{b \in \mathcal{B}} f_{bj}(\Gamma) b + d\psi,$$

we find polynomials $f_{bj}(\Gamma)$ with $\deg_{\Gamma} f_{bj} \leq \kappa j$. Lemma 2 of [7] implies that $\text{ord}(f_{bj}(\gamma)) \geq -(3 + \log_2(j + g + 1))$ for every $\gamma \in \mathbb{S}$, and combining this with Lemma 5 we find the same inequality for $\text{ord}(f_{bj})$. It is clear that as the valuations of the coefficients of the original expression grow linearly, we can ignore this logarithmic surplus of the reductions and hence suppose that the f_{bj} are integral. If we write

$$\tau = \sum_{j=0}^{\infty} s_j(\Gamma) X^j Y dX \equiv \sum_{b \in \mathcal{B}} \left(\sum_{j=0}^{\infty} s_j f_{bj} \right) b,$$

then we must show that $\sum_j s_j f_{bj} \in S$. We will prove that with $s_j f_{bj} = \sum_t \alpha_{tj}(\Gamma) \tilde{r}(\Gamma)^t$ an inequality $\text{ord}(\alpha_{tj}) \geq \varepsilon(|t| + j)$ holds for some $\varepsilon > 0$ and all t and j except precisely one case, namely $t = 1$ and $j = 0$. Expanding f_{bj} ‘in \tilde{r} ’ gives $f_{bj} = \sum_{\ell=0}^{Cj} \phi_{\ell j} \tilde{r}^{\ell}$, where $C = \lceil \kappa/\rho' \rceil$ and the polynomials $\phi_{\ell j}(\Gamma)$ are integral. When we multiply s_j with f_{bj} , a general term of the product is

$$\sum_{i+\ell=t} s_{ij} \phi_{\ell j} \tilde{r}^t.$$

The degree of $s_{ij} \phi_{\ell j}$ is at most $2\rho' - 2$, hence with Euclidean division written as $s = [s/\tilde{r}] \cdot \tilde{r} + (s \bmod \tilde{r})$ we have

$$\alpha_{tj} = \sum_{i+\ell=t} (s_{ij} \phi_{\ell j} \bmod \tilde{r}) \tilde{r}^t + \sum_{i+\ell=t-1} \left[\frac{s_{ij} \phi_{\ell j}}{\tilde{r}} \right] \tilde{r}^t.$$

The fact that \tilde{r} is integral and has a unit in \mathbb{Z}_q as leading coefficient implies that $[s/\tilde{r}]$ and $(s \bmod \tilde{r})$ have valuation not lower than $\text{ord}(s)$, so

$$\text{ord}(\alpha_{tj}) \geq \delta \left(j + \min_{\ell=0}^{Cj} (|t - \ell|, |t - 1 - \ell|) \right). \quad (4)$$

For $t \geq 2Cj + 2$ we have that the minimum in (4) is at least $|t|/2$, hence $\text{ord}(\alpha_{tj}) \geq \delta(j + |t|/2)$. For $t \leq 0$ we see immediately that $\text{ord}(\alpha_{tj}) \geq \delta(j + |t|)$, so suppose $0 < t < 2Cj + 2$. Excluding the case $(t = 1, j = 0)$ we have then $(2C + 2)j \geq |t|$, so that

$$\text{ord}(\alpha_{tj}) \geq \delta j = \delta \left(\frac{1}{2C+3} j + \frac{2C+2}{2C+3} j \right) \geq \frac{\delta}{2C+3} (j + |t|).$$

Combining these inequalities with Lemmata 8 and 9 of [12] implies that $\sum_j s_j f_{bj} - \alpha_{1,0} \tilde{r} \in S$, hence $\sum_j s_j f_{bj} \in S$.

For proving that ψ , coming from the exact differential $d\psi$, can also be chosen in T , we

need similar estimates using the full form of congruence (2). Indeed, we have

$$\begin{aligned} & \left(X^k(2f' + hh') + \frac{k}{3}X^{k-1}(4f + h^2) \right) Y dX = \\ & \frac{1}{2}d \left(\frac{X^k}{3}(4f + h^2)(2Y + h) \right) - d \int \left[\frac{X^k}{2}h(2f' + hh') + \frac{k}{6}X^{k-1}h(4f + h^2) \right] dX, \end{aligned}$$

as can be verified by using the equality $(2Y + h)^2 = 4f + h^2$. \square

2.3. The differential equation.

In this section we will construct the following commutative diagram and derive an important differential equation from it:

$$\begin{array}{ccc} H_{MW}^- & \xrightarrow{\nabla} & H_{MW}^- d\Gamma \\ \downarrow F_2 & & \downarrow F_2 \\ H_{MW}^- & \xrightarrow{\nabla} & H_{MW}^- d\Gamma. \end{array} \quad (5)$$

Let us start with the definition of the connection:

$$\nabla : H_{MW} \rightarrow H_{MW} d\Gamma : t \mapsto \frac{\partial t}{\partial \Gamma} d\Gamma, \quad \text{with} \quad \nabla(XdX) := XdXd\Gamma,$$

$$\nabla(YdX) = \dot{Y}dXd\Gamma := \frac{fh - 2f\dot{h} + (2\dot{f} + h\dot{h})Y}{4f + h^2} dXd\Gamma.$$

Similar computations as in the case of the differential d show that $\frac{\partial}{\partial \Gamma}$ and ∇ are well defined on T respectively H_{MW}^\pm .

The map $F_2 : T \rightarrow T$ represents a lift of the Frobenius automorphism $x \mapsto x^2$ in characteristic 2 and is defined as σ on \mathbb{Q}_q , $X \mapsto X^2$, $\Gamma \mapsto \Gamma^2$ and Y maps to the unique solution $F_2(Y)$ in T of $F_2(Y)^2 + h^\sigma F_2(Y) - f^\sigma = 0$ that is congruent to Y^2 modulo 2. Proposition 11 will imply that with this definition $F_2(Y)$ actually lies in T . We extend F_2 with $dX \mapsto d(X^2) = 2XdX$ and similarly $d\Gamma \mapsto 2\Gamma d\Gamma$. In order to prove that F_2 is also well defined on the quotient module H_{MW} it suffices to verify that F_2 commutes with the differential operator d , which is easily done. For the diagram above we need that H_{MW}^- is an invariant subspace under the action of F_2 , and this follows from the following lemma.

LEMMA 7. *The sum $\iota(F_2(YdX)) + F_2(YdX)$ is exact, hence for each $b \in \mathcal{B}$ we have $\iota(F_2(b)) = -F_2(b)$.*

Proof. Our proof is rather technical, we will use some sequence W_k from the Newton iteration as in [7], for which the approximation $F_2(Y) \equiv W_k \pmod{2^k}$ holds. Note that this implies that $F_2(YdX) \equiv 2XW_k dX \pmod{2^k}$. We define j on T by $j(t) := \iota(t) + t$, so $j(\alpha + \beta Y) = 2\alpha - h\beta$. We will show inductively for $k \geq 1$ that

$$j(W_k) = \iota(W_k) + W_k \equiv -h^\sigma \pmod{2^k}, \quad (6)$$

which implies that $\iota(F_2(Y)) + F_2(Y) = -h^\sigma$. We note that this equality is not really unexpected as $\iota(F_2(Y))$ satisfies the same quadratic equation as $F_2(Y)$ and $-h^\sigma$ is the sum of the two ‘roots’ of this equation.

As $W_1 = f - hY$, we find the induction basis $j(W_1) = 2f + h^2 \equiv -h^\sigma \pmod{2}$. Suppose that (6) holds for W_k , so $j(W_k) = -h^\sigma + 2^k \delta$ for some integral $\delta \in T$. Define now $\tilde{W}_k :=$

$W_k + 2^k Y \delta / h$, then $\tilde{W}_k \equiv W_k \pmod{2^k}$ and $j(\tilde{W}_k) = -h^\sigma$. In [7] the sequel value W_{k+1} is computed from W_k , but as $\tilde{W}_k \equiv W_k \pmod{2^k}$ we may take as well \tilde{W}_k for this:

$$h^2 W_{k+1} \equiv -\tilde{W}_k^2 + (h^2 - h^\sigma) \tilde{W}_k + f^\sigma \pmod{2^{k+1}}. \quad (7)$$

In the following α and β depend on k , but we suppress this to save notation. Write $\tilde{W}_k = \alpha + \beta Y$, then we have

$$j(\tilde{W}_k) = 2\alpha - h\beta = -h^\sigma, \quad (8)$$

$$\tilde{W}_k^2 = \alpha^2 + 2\alpha\beta Y + \beta^2 Y^2 = \alpha^2 + \beta^2 f + (2\alpha\beta - \beta^2 h)Y, \quad (9)$$

$$j(\tilde{W}_k^2) = 2(\alpha^2 + \beta^2 f) - h(2\alpha\beta - \beta^2 h), \quad (10)$$

$$\tilde{W}_k^2 \equiv f^\sigma - h^\sigma \tilde{W}_k \equiv f^\sigma - \alpha h^\sigma - (h^\sigma \beta)Y \pmod{2^k}. \quad (11)$$

Combining (9) and (11) and multiplying with 2 we find

$$2(\alpha^2 + \beta^2 f) \equiv 2(f^\sigma - \alpha h^\sigma) \pmod{2^{k+1}}, \quad (12)$$

and hence formulae (10), (12) and (8) give

$$j(\tilde{W}_k^2) \equiv 2(f^\sigma - \alpha h^\sigma) - h\beta(2\alpha - h\beta) \equiv 2(f^\sigma - \alpha h^\sigma) + h\beta h^\sigma \pmod{2^{k+1}}.$$

Using formula (8) once more implies that

$$j(\tilde{W}_k^2) \equiv 2f^\sigma - h^\sigma(2\alpha - h\beta) \equiv 2f^\sigma + (h^\sigma)^2 \pmod{2^{k+1}}.$$

Now we can compute $j(W_{k+1})$ from (7):

$$\begin{aligned} j(W_{k+1}) &\equiv \frac{1}{h^2} (-j(\tilde{W}_k^2) + (h^2 - h^\sigma)j(\tilde{W}_k) + 2f^\sigma) \pmod{2^{k+1}} \\ &\equiv \frac{1}{h^2} (-2f^\sigma - (h^\sigma)^2 - h^2 h^\sigma + (h^\sigma)^2 + 2f^\sigma) \equiv -h^\sigma \pmod{2^{k+1}}, \end{aligned}$$

which proves (6). □

It is possible to prove this lemma on a more conceptual level in the following way: lifting endomorphisms from the coordinate ring of the curve in characteristic 2 to the Monsky-Washnitzer cohomology is functorial, and as Frobenius commutes with the involution below, it will also commute in the characteristic zero case.

The fact that diagram (5) is commutative follows for example from the fact that Frobenius and ∇ commute on power series. We can derive from this diagram the central differential equation. Let $F(\Gamma)$ be the matrix of the operator F_2 on H_{MW}^- , given by $F_2(b_i) = \sum_k F_{ik} b_k$, and analogously let $G(\Gamma)$ be the matrix of ∇ . Using the relation $\nabla \circ F_2 = F_2 \circ \nabla$ on basis elements the following equation is easily obtained:

$$\dot{F}(\Gamma) + F(\Gamma)G(\Gamma) = 2\Gamma G^\sigma(\Gamma^2)F(\Gamma). \quad (13)$$

We will come back later to the problem of solving this equation in a decent way.

Suppose now that we use the same lift to some \mathbb{Q}_q^n (including $\Gamma \leftarrow \gamma$, namely $h(X) = h(X, \gamma)$ and $f(X) = f(X, \gamma)$) in the algorithm of Denef and Vercauteren as we did here. It is then clear that if $F(0)$ equals their Frobenius in $\Gamma = 0$, the same will hold for $F(\gamma)$ for every $\gamma \in \mathbb{S}$ because $F(\Gamma)$ is uniquely determined by (13) and $F(0)$.

3. Behaviour of matrices

In this section we will keep the notation introduced throughout Section 2. The theory in the foregoing section shows that the matrix of Frobenius $F(\gamma)$ for some $\gamma \in \mathbb{S}$, a specialisation of the solution of (13), can be computed by working over a small field (for finding $F(0)$) and solving the differential equation. Suppose that $\bar{\gamma} \in \mathbb{F}_{q^n}$, then we will explain in Section 4 that we have to compute $F(\Gamma)$ modulo 2^N and Γ^{N_Γ} for well-chosen N and N_Γ , both $O(n)$. There is an obvious way to find $F(\Gamma)$: calculate first an approximation of the matrix $G(\Gamma)$ of the connection ∇ , and use then a recursive computation in order to recover $F(\Gamma)$ from equation (13). We will now indicate why this is not a good idea, and in Section 3.1 we explain an alternative approach that does give interesting results.

The first row of the matrix $G(\Gamma)$ is determined by the reduction of ∇b_0 , which equals

$$\nabla(YdX) = \frac{fh - 2f\dot{h}}{4f + h^2} dXd\Gamma + \frac{2\dot{f} + h\dot{h}}{4f + h^2} YdXd\Gamma =: (\alpha(X, \Gamma) + \beta(X, \Gamma)Y)dXd\Gamma.$$

We know that $\nabla(YdX) \in H_{MW}^- d\Gamma$, and the reduction formulae (1) and (3) show then that $\alpha(X, \Gamma)dXd\Gamma$ will be cancelled by the appearing $IdX/(rH)$ in (3). So we are only interested in $\beta(X, \Gamma)Y$ and compute

$$\beta(X, \Gamma) = \frac{1}{h^2} \cdot \frac{2\dot{f} + h\dot{h}}{1 - (-4f/h^2)} = \frac{2\dot{f} + h\dot{h}}{h^2} \sum_{i=0}^{\infty} \left(\frac{-4f}{h^2} \right)^i. \quad (14)$$

This is an infinite power series in $1/h$ and hence in $1/H$, which converges so slowly that it has $O(n)$ terms if we work modulo 2^N . In order to express ∇b_0 in the basis $\mathcal{B} = \{b_i\}$, we hence have to use $O(n)$ times formula (3), and as a consequence the approximated $G_{0,0}$, the coefficient of b_0 in ∇b_0 , would be a power series of length $O(n)$ in $1/\tilde{r}$. Solving (13) in an inductive manner using formula (26) requires a representation of $G(\Gamma)$ as power series around zero, and such a representation needs also $O(n)$ terms if we work modulo 2^N . We conclude that computing $F(\Gamma) = \sum_k F_k \Gamma^k$ requires for each F_k a sum of $O(n)$ matrices with accuracy (and hence size) $O(n)$ yielding a total complexity of about $O(n^3)$ bit operations. Even worse is that in the expansion of (14) we have to express f^i as a ‘polynomial in H ’, say $f^i = \sum_j f_{ij} H^j$ with $\deg_X f_{ij} < \deg_X H$. In general this will give $\deg_\Gamma f_{ij} = O(i\kappa)$, and hence representing $\nabla(YdX)$ in a form suitable for using formula (3) could already require bit space of size cubic in n .

Besides a way to avoid the above problems, we will give in this section also an important estimate for $F(\Gamma)$. It is worth noting that in the odd characteristic case in [12] a similar problem arose, but there it was sufficient to multiply G with the resultant $r(\Gamma)$. In the current situation, the solution is more complicated.

3.1. Rewriting the matrix of the connection.

Define $v := 4f + h^2$ and $u := v'/2 = 2f' + hh'$. We construct a new basis for H_{MW}^- as $d_i := vb_i$; the fact that this is a basis follows from Proposition 9 below. The idea is that — as v arises as denominator in ∇b_i — the basis $\{d_i\}$ gives in some sense a nicer matrix for the connection. Consider the following matrices, where the right hand sides are obtained by reduction using formulae (2) and (3). By (b_i) we mean a column vector of length $2g$

with b_0 on top.

$$(d_i) = B \cdot (b_i), \quad (15)$$

$$\begin{aligned} \nabla(b_i) &= G \cdot (b_i) d\Gamma, \\ \nabla(d_i) &= D \cdot (b_i) d\Gamma. \end{aligned} \quad (16)$$

Here (15) and (16) define the matrices B and D . As follows from the preceding section, the entries of G are elements of S and it is not hard to see that the entries of B and D are polynomials in Γ over \mathbb{Q}_q . Using these relations and the equality $\nabla \circ d = d \circ \nabla$ we find

$$D \cdot (b_i) d\Gamma = \nabla(d_i) = \dot{B} \cdot (b_i) d\Gamma + B \cdot \nabla(b_i) = \dot{B} \cdot (b_i) d\Gamma + B \cdot G \cdot (b_i) d\Gamma$$

or in conclusion $D = \dot{B} + B \cdot G$.

3.2. Adaptation of the differential equation

If we combine the formula $D = \dot{B} + BG$ with the differential equation, we can find an equivalent equation where only polynomials of bounded degree — see Lemma 8 — appear. We can however even go further, namely as follows from Proposition 11 we need in fact $r(\Gamma)^M F(\Gamma)$ for some positive integer M . Let $R(\Gamma) := \det(B(\Gamma))$ and

$$K(\Gamma) := r(\Gamma)^M R(\Gamma) F(\Gamma) B(\Gamma)^{-1}, \quad (17)$$

then we can find a ‘small’ differential equation and a boundary condition $K(0) = K_0$ for $K(\Gamma)$. In Note 12 we will argue why we need the factor $R(\Gamma)$ in (17).

We recall that σ acts as squaring on Γ and X . The notation $B^\sigma(\Gamma^2)$ and the shorthand B^σ will both stand for the matrix obtained from $B(\Gamma)$ by the action of σ on the coefficients and on Γ , and similar for the other matrices. We start with $\dot{F} + FG = 2\Gamma G^\sigma F$, hence multiplying with B^σ on the left will remove G^σ :

$$B^\sigma \dot{F} + B^\sigma F G = 2\Gamma(D - \dot{B})^\sigma F.$$

Next we substitute $F = r^{-M} R^{-1} K B$, which after multiplication with $r^{M+1} R^2$ leads to

$$(rRB^\sigma) \dot{K} B + (rRB^\sigma) K D + (-(M\dot{r}R + r\dot{R})B^\sigma + 2\Gamma rR(\dot{B} - D)^\sigma) K B = 0. \quad (18)$$

An important property of this equation is that all coefficients consist of polynomials of low degree. As Proposition 9 will show, $B(0)$ is invertible, which will allow us to compute an approximate solution in $\mathbb{Q}_q[[\Gamma]]$ modulo a certain power of 2 and Γ for K in (18) using induction. Write $K = \sum_i K_i \Gamma^i$, where K_0 is known, then we can find all K_{k+1} one by one from K_k, K_{k-1}, \dots by looking at the coefficient of Γ^k . Finally $r^M R F$ is recovered as $K B$ and $r^M F$ is immediately deduced from it.

3.3. Behaviour of B and D .

In this section we prove a few important results about the structure of the matrices B and D . The first lemma provides bounds on the degree and the valuation of these matrices.

LEMMA 8. *For every i, j we have $\deg_\Gamma B_{ij} \leq (2g+2)\kappa$ and $\text{ord}_2(B_{ij}) \geq -(3 + \lfloor \log_2(5g+1) \rfloor)$, and also $\deg_\Gamma D_{ij} \leq (2g+1)\kappa - 1$ and $\text{ord}_2(D_{ij}) \geq -(3 + \lfloor \log_2(5g) \rfloor)$.*

Proof. First we consider B . We have for every i the equivalence

$$(4f + h^2)X^i Y dX \equiv \sum_{j=0}^{2g-1} B_{ij} X^j Y dX.$$

The reduction formula (2) has to be applied at most $2g + 1$ times and each time \deg_{Γ} increases at most by κ . Bounding the denominator naively would give the following product of valuation exactly $2g + 1$:

$$P := \prod_{m=0}^{2g} \left(2(2g+1) + \frac{4m}{3} \right). \quad (19)$$

However, the use of Lemma 2 of [7] gives the better logarithmic bound mentioned above. The results for D can be proven with similar estimates. \square

The following proposition implies that $B(\Gamma)$ is invertible as matrix over S . Indeed, Lemma 19 of [12] shows that if $\text{ord}_2(s(\gamma)) = 0$ for some $s \in S$ and all $\gamma \in \mathbb{S}$, then $1/s \in S$. If we apply this to $s(\Gamma) = \det(B(\Gamma))$ we find that $1/s(\Gamma)$ multiplied with the adjoint matrix of $B(\Gamma)$ is indeed defined over S and equal to $B(\Gamma)^{-1}$.

PROPOSITION 9. For every $\gamma \in \mathbb{S}$ we have $\text{ord}_2(R(\gamma)) = \text{ord}_2(\det(B(\gamma))) = 0$.

Proof. We will prove in a first step that, with P defined in (19):

$$\det(B) \cdot P = \text{Res}_X(u, v), \quad (20)$$

and afterwards some property of the resultant will show that for every $\gamma \in \mathbb{S}$ this last resultant has the same valuation $2g + 1$ as P , which gives the proposition.

Define $\alpha_j := X^j u + (j/3)X^{j-1}v$ for $j \geq 0$, then formula (2) reads $\alpha_j Y dX \equiv 0$. It is easy to verify that the leading term of α_j equals $(2(2g+1) + 4j/3)X^{j+2g}$. Let m be a polynomial in the variables $X, \mu_0, \dots, \mu_{2g}, \lambda_0, \dots, \lambda_{2g-1}$ with coefficients in $\mathbb{Q}_q[\Gamma]$, and suppose m is homogenous of degree 1 in the set of variables $\{\mu_i, \lambda_i\}$ and has degree at most $4g$ in X . We can associate with m a $(4g+1) \times (4g+1)$ matrix M over $\mathbb{Q}_q[\Gamma]$ in the following way. The entry M_{ij} equals the coefficient in m of $\mu_{2g+1-i}X^{4g+1-j}$ for $i \leq 2g+1$, and for $2g+2 \leq i$ the entry M_{ij} is given by the coefficient of $\lambda_{4g+1-i}X^{4g+1-j}$. Schematically this becomes the following (interpret $\mu_i X^j$ as ‘the coefficient of $\mu_i X^j$ in m ’ etc.):

$$M = \begin{pmatrix} \mu_{2g}X^{4g} & \mu_{2g}X^{4g-1} & \dots & \mu_{2g}X^0 \\ \vdots & \vdots & & \vdots \\ \mu_0X^{4g} & \mu_0X^{4g-1} & \dots & \mu_0X^0 \\ \lambda_{2g-1}X^{4g} & \lambda_{2g-1}X^{4g-1} & \dots & \lambda_{2g-1}X^0 \\ \vdots & \vdots & & \vdots \\ \lambda_0X^{4g} & \lambda_0X^{4g-1} & \dots & \lambda_0X^0 \end{pmatrix}.$$

We start with the matrix M associated to the polynomial

$$m := \lambda_0 X^0 v + \lambda_1 X^1 v + \dots + \lambda_{2g-1} X^{2g-1} v + \mu_0 \alpha_0 + \mu_1 \alpha_1 + \dots + \mu_{2g-1} \alpha_{2g-1} + \mu_{2g} \alpha_{2g}.$$

By means of the transformation $\lambda_j \leftarrow \lambda_j - ((j+1)/3)\mu_{j+1}$, which corresponds to an elementary row operation, it is easy to see that the determinant of M is precisely the resultant $\text{Res}_X(u, v)$.

The reduction process applied to the basis elements $d_j = vb_j$ gives rise to formulae of the form

$$X^j v Y dX = B_j(X) Y dX + \sum_{i=0}^{j+1} \beta_{ij} \alpha_i Y dX,$$

for $j = 0, \dots, 2g-1$, $\beta_{ij} \in \mathbb{Q}_q[\Gamma]$ and $\deg_X B_j(X) \leq 2g-1$. The coefficients of B_j are exactly the entries of the j th row of the matrix B . If we substitute these expressions in our polynomial m , we find

$$m = \lambda_0 B_0 + \dots + \lambda_{2g-1} B_{2g-1} + \left(\mu_0 + \sum_{j=0}^{2g-1} \lambda_j \beta_{0,j} \right) \alpha_0 + \\ \left(\mu_1 + \sum_{j=0}^{2g-1} \lambda_j \beta_{1,j} \right) \alpha_1 + \left(\mu_2 + \sum_{j=1}^{2g-1} \lambda_j \beta_{2,j} \right) \alpha_2 + \dots + \left(\mu_{2g} + \sum_{j=2g-1}^{2g-1} \lambda_j \beta_{2g,j} \right) \alpha_{2g}.$$

With the substitution $\mu_i \leftarrow \mu_i + \sum_{j=\max(i-1,0)}^{2g-1} \lambda_j \beta_{i,j}$ again the determinant of the associated matrix does not change, and the result of this substitution is

$$m_1 := \lambda_0 B_0 + \dots + \lambda_{2g-1} B_{2g-1} + \mu_0 \alpha_0 + \dots + \mu_{2g} \alpha_{2g},$$

with M_1 as associated matrix, hence $\det(M) = \det(M_1)$. Now the matrix M_1 has the following form:

$$M_1 = \begin{pmatrix} \delta & \star \\ 0 & \tilde{B} \end{pmatrix},$$

where δ is the upper left $(2g+1) \times (2g+1)$ submatrix of M_1 , and the structure of the polynomials α_j implies that it is in uppertriangular form with determinant P . The $(2g) \times (2g)$ submatrix \tilde{B} equals the matrix B with the row and column order reversed. This concludes the proof of the equality $\det(B) \cdot P = \text{Res}_X(u, v)$. We now prove a short lemma needed further on.

LEMMA 10. *Let R be a ring and $\alpha, \beta, \gamma \in R[X]$ with $\deg \beta = \deg(\beta + \alpha\gamma)$, then $\text{Res}_X(\alpha, \beta) = \text{Res}_X(\alpha, \beta + \alpha\gamma)$.*

This lemma remains true without the condition on the degree, given that α is monic. Otherwise the resultants agree up to an appropriate power of the leading coefficient of α , but we will not use this more general result.

Proof. The matrix defining the second resultant can be achieved from the matrix defining the first resultant by adding to the rows according to β suitable multiples of the rows of α . These elementary row operations do not change the determinant. \square

We continue with the proof of Proposition 9 and show that $\text{Res}_X(u, v)$ has valuation $2g+1$ for every $\gamma \in \mathbb{S}$. So from now on we work with a concrete $\gamma \in \mathbb{S}$, hence $f = f(X, \gamma)$ etc. If $H = 1$ the result can be verified directly, so we suppose that $\deg H \geq 1$. Using $v = 4f + h^2 = H \cdot (4Q_f + h^2/H)$ and the multiplicative property of the resultant, we can write

$$\text{Res}_X(v, u) = \text{Res}_X(H, 2f' + hh') \cdot \text{Res}_X(4Q_f + h^2/H, 2f' + hh').$$

By the lemma and the fact that H and $Q_f H'$ are relatively prime over the residue field $\mathbb{F}_q(\tilde{\gamma})$ we have that the first factor has valuation $\deg H$. Define $\tilde{h} := h/H$, then we have — as can be checked by writing \tilde{h} as a product of linear factors over $\mathbb{Q}_q^{\text{alg cl}}$ — that \tilde{h} is a divisor of $H\tilde{h}'$ with integral quotient $\alpha \in \mathbb{Z}_q^{\text{alg cl}}[X]$. The lemma implies that

$$\text{Res}_X(4Q_f + \tilde{h}h, 2f' + hh') = \text{Res}_X(4Q_f + \tilde{h}h, 2f' + hh' - (H' + \alpha)(4Q_f + \tilde{h}h)) \\ = \text{Res}_X(4Q_f + \tilde{h}h, 2Q_f' H - 2Q_f H' - 4Q_f \alpha).$$

Note that the coefficient of X^{2g} of the second polynomial in these equalities is always congruent to 2 modulo 4, and hence nonzero.

The last resultant above equals $2^{\deg Q_f}$ times

$$\text{Res}_X(4Q_f + \tilde{h}h, Q'_f H - Q_f H' - 2Q_f \alpha),$$

and it is immediate that the leading coefficient of $Q'_f H - Q_f H' - 2Q_f \alpha \pmod 2$ equals 1. By looking at the Sylvester determinant and noting that, although the degree of the first polynomial can decrease, no problem modulo 2 arises, we see that

$$\text{Res}_X(4Q_f + \tilde{h}h, Q'_f H - Q_f H' - 2Q_f \alpha) \equiv \text{Res}_X(\tilde{h}h, Q'_f H - Q_f H') \pmod 2.$$

Again using the lemma we find $\text{Res}_X(\tilde{h}h, -Q_f H')$ modulo 2, which is nonzero by construction. As conclusion we see that $\text{Res}_X(v, u) = \text{Res}_X(u, v)$ has valuation exactly $\deg Q_f + \deg H = 2g + 1$. \square

A consequence of this proposition is an estimate on B^{-1} . Indeed, suppose $2^\varepsilon B$ is integral, then the fact that the inverse of a matrix equals its adjoint matrix divided by the determinant gives that the valuation of B^{-1} is at least $-(2g - 1)\varepsilon$. Together with Lemma 8 we can conclude that, defining $\beta' := (2g - 1)(3 + \lfloor \log_2(5g + 1) \rfloor) = O(g \log g)$, we have $\text{ord}_2(B^{-1}) \geq -\beta'$. Formula (20) in the proof above also implies that $\deg_\Gamma R(\Gamma) = \deg_\Gamma(\det(B(\Gamma))) \leq 4g\kappa$.

3.4. On the convergence rate of $F(\Gamma)$.

A crucial point in all p -adic algorithms is that it suffices to work modulo a certain power of p . As we have to work in our deformation algorithm also modulo a power of Γ , it is important to know which power is needed, depending on the required precision in p . The following proposition gives such a result. Recall the definition of κ and \tilde{D} in Section 2.1.

PROPOSITION 11. *Let $N \in \mathbb{N}$ and $f(\Gamma)$ be an entry of $F(\Gamma)$, reduced modulo 2^N . Then there exist explicit constants $\chi_1 = O(N(\tilde{D} + \log g))$ and $\chi_2 = O(g\kappa N\tilde{D})$ such that the expression $r^{\chi_1} f(\Gamma) \pmod{2^N}$ is a polynomial of degree less than χ_2 . Also we have an explicit constant $\varphi = O(\log g)$ such that $\text{ord}_2(F(\Gamma)) \geq -\varphi$.*

Proof. Recall from Section 3.2 in [7] the approximation W_k to $F_2(Y)$, also used in the proof of Lemma 7 above. By defining $\alpha_k(X, \Gamma)$, $\beta_k(X, \Gamma)$ such that $W_k = \alpha_k + \beta_k Y$; $\Delta_{\alpha, k} := (\alpha_k - \alpha_{k-1})/2^{k-1}$ and similarly $\Delta_{\beta, k}$ we can compute $c^2 H^{2\tilde{D}} W_k$ from the following formula of [7]:

$$c^2 H^{2\tilde{D}} W_k \equiv Q_h^2 \cdot \{-W_{k-1}^2 + (h^2 - h^\sigma)W_{k-1} + f^\sigma\} \pmod{2^k}.$$

This gives as result, where $i, j \geq 1$ in all sums:

$$\begin{aligned} c^2 H^{2\tilde{D}} W_k &\equiv -Q_h^2 \sum_{i < j, i+j \leq k} 2^{i+j-1} (\Delta_{\alpha, i} \Delta_{\alpha, j} + (f - hY) \Delta_{\beta, i} \Delta_{\beta, j}) \\ &- Y Q_h^2 \sum_{i+j \leq k} 2^{i+j-1} \Delta_{\alpha, i} \Delta_{\beta, j} - Q_h^2 \sum_{2i \leq k+1} 2^{2(i-1)} (\Delta_{\alpha, i}^2 + (f - hY) \Delta_{\beta, i}^2) \\ &+ (h^2 - h^\sigma) Q_h^2 \sum_{i \leq k-1} 2^{i-1} (\Delta_{\alpha, i} + \Delta_{\beta, i} Y) + Q_h^2 f^\sigma \pmod{2^k}. \end{aligned} \quad (21)$$

We know that $W_k = \alpha_k + Y\beta_k \in T$ and can hence express α_k and β_k as overconvergent power series in X and H^{-1} with coefficients in S . We will not go into details in the easy case where $\deg_X H = 0$, but if $\deg_X H \geq 1$ we can write α_k and β_k also as power series in H and H^{-1} . It is not hard to show inductively that in this form for $k \geq 2$ the coefficients of $c^{4k-6}W_k$ are polynomials in (X) and in Γ . We will prove that for $k \geq 2$ the coefficients in $c^{4k-6}W_k$ as in (21) have \deg_Γ at most $Ak - B$, with $A := 2\omega$, $B := 3\omega$, and (recall that $\eta = \deg_\Gamma H$ and $hQ_h = cH^{\tilde{D}}$)

$$\omega := 2\kappa + \deg_\Gamma Q_h^2 + [(\deg_X(f^2 Q_h^2))/\deg_X H]\eta + 3\eta + 2\kappa.$$

Here $\omega - 3\eta - 2\kappa \leq 2A - B$ is a bound for the degree in Γ in c^2W_2 , as can be verified by a direct computation. To prove the bound $Ak - B$ we use induction and consider each term in the formula for W_k above. For instance, for $c^{4k-6}Q_h^2\Delta_{\alpha,i}\Delta_{\alpha,j}$ with $j > i \geq 2$ we find as a bound (note that $\deg_\Gamma c \leq \kappa$ and $A \geq 4\kappa$)

$$\begin{aligned} & Ai - B + Aj - B + \deg_\Gamma Q_h^2 + (\deg_X Q_h^2/\deg_X H + 2)\eta + [4(k - (i + j)) + 4]\kappa \\ & \leq A(i + j) + A(k - (i + j)) - B + \deg_\Gamma Q_h^2 + (\deg_X Q_h^2/\deg_X H + 2)\eta + 4\kappa - B \leq Ak - B. \end{aligned}$$

The term with η comes from expanding polynomials in X as series in H . As ω is also a bound for W_1 and $i, j \leq k - 1$ we have our estimate for all i, j . For the other terms a similar computation works. For example, for $c^{4k-6}Q_h^2 f \Delta_{\beta,i}^2$ we have, as $2i \leq k + 1$,

$$\begin{aligned} & 2Ai - 2B + \deg_\Gamma Q_h^2 + \kappa + [\deg_X(fQ_h^2)/\deg_X H + 3]\eta + [4k - 8 - (4(2i) - 12)]\kappa \\ & \leq Ak - B. \end{aligned}$$

In a second step we have to reduce $c^{4k-6}W_k$ in the cohomology. As $F_2(Y) \in H_{MW}^-$ we can confine ourselves to the part with Y in it. First we take some $g(\Gamma)X^t Y dX$, and reducing this by using formula (2) adds less than $t\kappa$ to the degree in Γ . Lemma 1 of [7] shows that $X^t Y dX$ has possible nonzero coefficient modulo 2^M only if $t \leq (aM + b)s$ with $as = 2(2g + 1 - 2\deg_X h)$ and $bs = 7\deg_X h - 3(2g + 1)$. Take M such that $M - (3 + \log_2((aM + b)s + g + 1)) \geq N$, then clearly $M = O(N + \log g)$ and Lemma 2 of [7] gives that it is enough to compute W_M for finding $F_2(Y) \bmod 2^N$ in H_{MW}^- , at least for the part without denominators H . Thus the worst possible \deg_Γ comes from the term $c^{4M-6}VH^{aM+b}$, which gives a degree in Γ of at most $AM - B$. During the reduction an extra degree in Γ of $(aM + b)s\kappa$ can occur, and taking everything together we find that the contribution of the part without denominator H — after multiplication with r^{4M-6} , a multiple of c^{4M-6} — is at most $AM - B + (aM + b)s\kappa + (4M - 6)\rho$.

For the part of $F_2(Y)$ which has H as denominator we consider terms of the form $(V/H^\ell)Y dX$ for $\ell > 0$. During the reduction from $1/H^\ell$ to $1/H^{\ell-1}$ the degree in X increases by at most $s + 2g$, the degree in Γ by at most $(2g + 2)\kappa$, and a denominator $r(\Gamma)$ appears. In the end we also have to reduce as in the previous paragraph, starting from \deg_X at most $\ell(s + 2g)$. Let $\tilde{a} := 4\tilde{D}$ and $\tilde{b} := -6\tilde{D}$, so that Lemma 1 of [7] implies that modulo $2^{\tilde{M}}$ we only need $\ell \leq \tilde{a}\tilde{M} + \tilde{b}$. Then with \tilde{M} such that $\tilde{M} - (3 + \log_2(\tilde{M} + 1)) \geq N$ we have that $\tilde{M} = O(N)$ and from Lemma 3 of [7] it follows that $W_{\tilde{M}}$ suffices for this part. Hence the worst case here is the denominator $H^{\tilde{a}\tilde{M} + \tilde{b}}$, where \deg_Γ is at most $A\tilde{M} - B$. All together this gives for the numerator a degree in Γ of at most $A\tilde{M} - B + (2g + 2)\kappa(\tilde{a}\tilde{M} + \tilde{b}) + (\tilde{a}\tilde{M} + \tilde{b})(s + 2g)\kappa$, and a denominator $r^{\tilde{a}\tilde{M} + \tilde{b} + 4\tilde{M} - 6}$.

It is now easy to find the bounds from the proposition: the denominator is r to the power $\max(\tilde{a}\tilde{M} + \tilde{b} + 4\tilde{M} - 6; 4M - 6)$ with $\tilde{a}, \tilde{b} = O(\tilde{D})$ and $\tilde{M} = O(N)$; and as bound χ_2 for the

degree of the numerator we find

$$\max \left\{ A\tilde{M} - B + (2g+2)\kappa(\tilde{a}\tilde{M} + \tilde{b}) + (\tilde{a}\tilde{M} + \tilde{b})(s+2g)\kappa, \right. \\ \left. AM - B + (aM+b)s\kappa + (4M-6)\rho \right\} + 1.$$

Using $A, B, \rho = O(g\kappa)$, $s = O(g)$ and as and bs as before the proposition follows.

We note that we should in fact look at $F_2(X^iY)$ for $i = 0, \dots, 2g-1$, but the possible increased \deg_Γ caused by this is absorbed in the rough estimates during the proof.

In order to determine φ we need to combine Lemmata 1, 2 and 3 of [7]. Choosing a modulus 2^k , Lemma 1 implies that the highest appearing degree of X in the Y -part of $F_2(Y)$ is less than $(4g+2)k+g$. Linked with Lemma 2 this part gives then a valuation bigger than

$$\min_{k \geq 0} (k-3 - \log_2((4g+2)k+2g+1)). \quad (22)$$

On the side with denominators we find as extremum $4\tilde{D}k - 6\tilde{D}$, and Lemma 3 then gives the lower bound

$$\min_{k \geq 0} (k-3 - \log_2(4\tilde{D}k - 6\tilde{D} + 1)). \quad (23)$$

Now we can take $-\varphi$ as the minimum of (22) and (23), and we see immediately that $\varphi = O(\log g)$. \square

Note 12. A corollary of Proposition 11 and Lemma 8 is that with $M = \chi_1$ we have that $K(\Gamma) \bmod 2^N$ as defined in (17) consists of polynomials of degree at most

$$\chi_2 + \deg_\Gamma(R(\Gamma) \cdot B(\Gamma)^{-1}) \leq \chi_2 + (2g-1)(2g+2)\kappa,$$

and $\text{ord}_2(K(\Gamma)) \geq -(\varphi + \beta')$. Note that $r(\Gamma)^M F(\Gamma) B(\Gamma)^{-1} \bmod 2^N$ does not need to have finite length, which is the reason why we multiply $B(\Gamma)^{-1}$ with $R(\Gamma)$. When implementing these results one finds that $F(\Gamma)^{-1}$, $B(\Gamma)^{-1}$ and the matrix of the big Frobenius actually have also very good 2-adic valuation¹, good enough to suggest a bound of $O(\log g)$ for them as well. In [6] a proof is given for the q th power Frobenius, but we do not know how to prove it for $F(\Gamma)^{-1}$ and $B(\Gamma)^{-1}$.

3.5. Error propagation in the inductive computation.

When solving the equation

$$(rRB^\sigma)\dot{K}B + (rRB^\sigma)KD + (-(MrR + r\dot{R})B^\sigma + 2\Gamma rR(\dot{B} - D)^\sigma)KB = 0, \quad K(0) = K_0 \quad (24)$$

in an inductive manner using equation (26), we could estimate the loss in accuracy in a naive way. However, already $\dot{K} = \sum_i iK_i\Gamma^{i-1}$ implies division by k for computing K_k , and hence at least $\text{ord}_2((N_\Gamma - 1)!) would be lost as accuracy, assuming that we work modulo Γ^{N_Γ} . It turns out to be possible to do better, as we will show in Theorem 13. Some form of this theorem has been found independently from the author by Gerkmann in [11].$

For every matrix $A(\Gamma)$ defined over $\mathbb{Q}_q[[\Gamma]]$ we write $A(\Gamma) = \sum_i A_i\Gamma^i$, hence $A(0) = A_0$. Let $-\varphi$ be the lower bound for the valuation $\text{ord}_2(F(\Gamma))$ found in Proposition 11, and $-\varphi_0$ a lower bound for $\text{ord}_2(F(\Gamma)^{-1})$. By Lemma 19 in [12] — the proof of which is also correct for $p = 2$ — we can take $\varphi_0 = \varphi(2g-1) + g$. Denote by \mathcal{K} the solution for K

¹This is also true for $F(\Gamma)^{-1}$ and the big Frobenius in odd characteristic.

of (24) obtained by working modulo 2^N and starting with $\mathcal{X}_0 = K_0 = r(0)^M R(0) F_0 B_0^{-1}$. The exact solution will be denoted by K , hence $K = r^M R F B^{-1}$. Finally we write $A_0 := r(0)^M R(0) F_0 = K_0 B_0$.

THEOREM 13. *With $\tilde{K} := 2^{-N}(\mathcal{X} - K) = \sum_i \tilde{K}_i \Gamma^i$ we have*

$$\text{ord}_2(\tilde{K}_i) \geq -(10g\varphi + 5g + 1) \cdot \lceil \log_2(i + 1) \rceil - \alpha,$$

where $\alpha := (12g - 1)(3 + \lceil \log_2(5g + 1) \rceil) + (8g + 1)\varphi + 4g$.

Proof. We will prove this theorem in a number of steps. Let us first define and recall some terms. For ease of notation we write $E := -(M\dot{r}R + r\dot{R})B^\sigma + 2\Gamma rR(\dot{B} - D)^\sigma$, equation (24) reads then

$$(rRB^\sigma)\dot{K}B + (rRB^\sigma)KD + EKB = 0.$$

We know the following bounds: from Lemma 8 follows that

$$\text{ord}_2(B) = \text{ord}_2(B^\sigma) \geq -\beta := -(3 + \lceil \log_2(5g + 1) \rceil), \quad (25)$$

and with β' such that $\text{ord}_2(B^{-1}) = \text{ord}_2((B^\sigma)^{-1}) \geq -\beta'$ as defined after the proof of Proposition 9 we have $\beta + \beta' = 2g\beta$. In the same way we have $\varphi + \varphi_0 = 2g\varphi + g$. Note that $\text{ord}_2(K) \geq -\varphi - \beta'$, $\text{ord}_2(K^{-1}) \geq -\varphi_0 - \beta$, $\text{ord}_2(A_0) \geq -\varphi$ and $\text{ord}_2(A_0^{-1}) \geq -\varphi_0$.

DEFINITION 14. Let A_i be for every $i \geq 0$ a $(2g \times 2g)$ -matrix over \mathbb{C}_2 and $x, y \in \mathbb{R}$. We say that the power series $\sum_i A_i \Gamma^i$ converges (x, y) -logarithmically if for all i

$$\text{ord}_2(A_i) \geq -x \cdot \lceil \log_2(i + 1) \rceil - y.$$

To shorten notation we will also write (x, y) -log instead of (x, y) -logarithmically.

LEMMA 15. *If $\sum_i A_i \Gamma^i$ and $\sum_i B_i \Gamma^i$ converge (x, y) - respectively (x', y') -logarithmically, then their product converges $(x + x', y + y')$ -log.*

Proof. The coefficient of Γ^k in the product is $\sum A_i B_j$, summed over $i + j = k$. Hence its valuation is at least

$$-x \lceil \log_2(i + 1) \rceil - x' \lceil \log_2(j + 1) \rceil - (y + y') \geq -(x + x') \lceil \log_2(k + 1) \rceil - (y + y'),$$

which gives the lemma. \square

LEMMA 16. *Let C be the (exact) solution of $\dot{C}B + CD = 0$ subject to $C(0) = B_0^{-1}$, then C converges $(\varphi + \varphi_0, \beta')$ -logarithmically, and for C^{-1} we find $(\varphi + \varphi_0, \beta)$ -log convergence.*

Proof. The matrix $\tilde{C} := CB$ gives in fact the solutions as Taylor expansions around zero of the equation $\nabla = 0$ or $\dot{\tilde{C}} + \tilde{C}G = 0$, with boundary condition $\tilde{C}(0) = 1$. From diagram (5) we can deduce the equality

$$\tilde{C}^\sigma(\Gamma^2)F(\Gamma) = F(0)\tilde{C}(\Gamma)$$

as at the end of Section 3 of [12]. Now exactly the same proof as for Proposition 20 in [12] gives that \tilde{C} converges $(\varphi + \varphi_0, 0)$ -logarithmically. As B^{-1} can be considered to have $(0, \beta')$ -log convergence, Lemma 15 gives the result. The estimate for $C^{-1} = B\tilde{C}^{-1}$ can be proven in a similar fashion. \square

We now give in Lemmata 17 and 18 an estimate on the error propagation for two ‘partial solutions’ of the equation. Note that we do not need these in the algorithm, only in this proof. A lemma with the flavour of the following one was first given by Lauder as Theorem 5.1 in [17], but we give a proof similar to our proof of Lemma 21 in [12]. Let C be the solution computed inductively using formula (26) modulo 2^N from the equation $\dot{C}B + CD = 0$ with $C(0) = B_0^{-1}$.

LEMMA 17. $2^{-N}(C - C)$ converges $(2\varphi + 2\varphi_0 + 1, \beta + 2\beta')$ -logarithmically.

Proof. It is easy to see (a formal argument will be given in the proof of Lemma 19) that C satisfies $\dot{C}B + CD = 2^N \mathcal{E}_1$ with \mathcal{E}_1 some matrix of power series in Γ with 2-adic integral coefficients. Let L be such that $2^N LC = C - C$. Then we can compute

$$2^N \mathcal{E}_1 = \dot{C}B + CD - \dot{C}B - CD = 2^N (\dot{L}CB + L\dot{C}B + LCD) = 2^N \dot{L}CB$$

and as a consequence $\dot{L} = \mathcal{E}_1 B^{-1} C^{-1}$. If we integrate \dot{L} we find as integration constant $L_0 = 0$, and hence

$$2^{-N}(C - C) = LC = \left(\int \mathcal{E}_1 B^{-1} C^{-1} d\Gamma \right) C.$$

As integrating is not worse than adding 1 to the logarithmic factor, we find the lemma. \square

Continuing with our proof of Theorem 13 we also need an estimate on the other ‘partial solution’. Let \mathcal{P} and P be the computed modulo 2^N resp. exact solution of $(rRB^\sigma)\dot{P} + EP = 0$ subject to $P(0) = I$, then a trivial computation shows that $K = PA_0C$ satisfies (24). Now Lemma 16 implies that $P = KC^{-1}A_0^{-1}$ converges $(\varphi + \varphi_0, \beta + \beta' + \varphi + \varphi_0)$ -logarithmically and the same holds for $P^{-1} = A_0CK^{-1}$. This follows from the lower bounds on the valuation of K, K^{-1}, A_0 and A_0^{-1} and Lemma 15. With a proof similar to that of Lemma 17 and using $(rRB^\sigma)\dot{P} + EP = 2^N \mathcal{E}_2$ we find the following:

LEMMA 18. $2^{-N}(\mathcal{P} - P)$ converges $(2\varphi + 2\varphi_0 + 1, 2\beta + 3\beta' + 2(\varphi + \varphi_0))$ -logarithmically.

The proof of the theorem can now be completed by estimating $\mathcal{K} - \mathcal{P}A_0C$ and $\mathcal{P}A_0C - K$ and summing these terms. For the first term we use the following lemma.

LEMMA 19. $2^{-N}(\mathcal{K} - \mathcal{P}A_0C)$ converges $(5\varphi + 5\varphi_0 + 1, 5\beta + 6\beta' + 5\varphi + 4\varphi_0)$ -logarithmically.

Proof. Denote the additive operator of (24) by Δ , hence (24) equals $\Delta K = 0$. We will first show how inductively computing a solution \mathcal{K} of $\Delta K = 0$ modulo 2^N can be modelled by an equality $\Delta \mathcal{K} = 2^N \mathcal{E}$ for some integral matrix \mathcal{E} . For each k we compute \mathcal{K}_k from

$$[r(0)R(0)B_0^\sigma k \mathcal{K}_k B_0 + f_k(\mathcal{K}_{k-1}, \mathcal{K}_{k-2}, \dots)] \Gamma^{k-1} = 2^N (\text{integral error matrix}) \Gamma^{k-1} \quad (26)$$

for some linear functions f_k . The sum over all these equations gives $\Delta \mathcal{K} = 2^N \mathcal{E}$.

Let L be defined such that $2^N PLA_0C = \mathcal{K} - \mathcal{P}A_0C$, then we compute

$$2^{-N}(\Delta \mathcal{K} - \Delta(\mathcal{P}A_0C)) = \Delta(PLA_0C) = rRB^\sigma P\dot{L}A_0CB. \quad (27)$$

Using the same integral as before and the fact that

$$\Delta(\mathcal{P}A_0C) = 2^N (rRB^\sigma \mathcal{P}A_0 \mathcal{E}_1 + \mathcal{E}_2 A_0 C B),$$

we find our result. Indeed, for $2^{-N}\Delta(\mathcal{P}A_0C)$ we find $(\varphi + \varphi_0, 2\beta + \beta' + 2\varphi + \varphi_0)$ -log convergence, and adding the inverse of the factors in the right hand side of (27) gives the lemma. \square

To end the proof of Theorem 13 we still have to control the difference $2^{-N}(\mathcal{P}A_0C - PA_0C)$. This can easily be done by adding a cross term:

$$2^{-N}(\mathcal{P}A_0C - PA_0C + PA_0C - PA_0C) = 2^{-N}(\mathcal{P} - P)A_0C + 2^{-N}PA_0(C - C).$$

The $(3\varphi + 3\varphi_0 + 1, 2\beta + 4\beta' + 3\varphi + 2\varphi_0)$ -logarithmic convergence of this difference is now clear, and taking the maximum of this result and the last lemma gives the theorem. Indeed, we have $K = PA_0C$ and

$$2^{-N}(\mathcal{K} - K) = 2^{-N}(\mathcal{K} - \mathcal{P}A_0C) + 2^{-N}(\mathcal{P}A_0C - PA_0C).$$

□

4. The algorithm

In this section we give a concrete presentation of the algorithm. We suppose that the polynomials $c(\Gamma)$, $H(X, \Gamma)$, $Q_f(X, \Gamma)$, $h(X, \Gamma)$ and $f(X, \Gamma)$ are given as explained in Section 2.1, where \mathbb{Q}_q is computed as in Section 5.1. The input of the algorithm is hence formed by these polynomials over $\mathbb{Z}_q = \mathbb{Z}_{2^a}$ and some parameter $\tilde{\gamma} \in \mathbb{F}_{q^n}$ which satisfies the resultant condition proven in Lemma 4. The output is the zeta function of the complete model of the hyperelliptic curve given by $Y^2 + \tilde{h}(X, \tilde{\gamma})Y = \tilde{f}(X, \tilde{\gamma})$, where we have projected the above polynomials modulo 2. We will suppose below that $\mathbb{F}_q[\tilde{\gamma}] = \mathbb{F}_{q^n}$. This is however not crucial, if $\tilde{\gamma}$ defines a smaller field then the zeta function over \mathbb{F}_{q^n} is easily derived from it. Indeed, if $Z(T)$ is the numerator of some zeta function over \mathbb{F}_q , then $\text{Res}_X(Z(X), X^k - T)$ is the numerator of the same zeta function over \mathbb{F}_{q^k} .

STEP 1. Compute the resultant $r(\Gamma) = c(\Gamma) \cdot \text{Res}_X(H(X, \Gamma), Q_f(X, \Gamma) \cdot H(X, \Gamma)')$. Let g be the genus and choose $M = \chi_1$ and χ_2 as in the proof of Proposition 11 with N defined as below. The value of φ can also be found in this proof. The constant α is defined in Theorem 13, $\kappa := \max\{\deg_\Gamma f, \deg_\Gamma h^2\}$, and we set

$$\begin{aligned} N_f &:= \left\lceil \log_2 \binom{2g}{g} + 1 + ang/2 \right\rceil, \\ N &:= N_f + (2g - 1)(3 + \lfloor \log_2(5g + 1) \rfloor) + an\varphi + 2gan\varphi, \\ N_\Gamma &:= \chi_2 + (2g - 1)(2g + 2)\kappa + 1, \\ N_2 &:= N + \alpha + (10g\varphi + 5g + 1)\lceil \log_2(N_\Gamma) \rceil. \end{aligned}$$

In Steps 2, 3 and 4 we will work modulo 2^{N_2} and Γ^{N_Γ} , and in Steps 5 and 6 modulo 2^N .

STEP 2. Compute the matrices B and D by using formula (2), and $R = \det(B)$ using equality (20).

STEP 3. Calculate $F(0)$ as explained in [7], but with the higher accuracy 2^{N_2} . Note that we need the *small* Frobenius, that is to say the 2nd power Frobenius.

STEP 4. Compute $K(\Gamma)$ in an inductive manner using formula (26) with starting condition $K_0 = r(0)^M R(0) F(0) B(0)^{-1}$.

STEP 5. Let $\tilde{\psi}(z)$ be the minimal polynomial of $\tilde{\gamma}$ over \mathbb{F}_q and $\psi(z)$ its Teichmüller modulus lift as explained in Section 5.1 below. Then $\mathbb{Q}_{q^n} = \mathbb{Q}_q[z]/\psi(z)$ and z is the Teichmüller lift of $\tilde{\gamma}$. Determine

$$F(z) = \frac{1}{r(z)\chi_1 R(z)} \cdot K(z) \cdot B(z).$$

STEP 6. Compute

$$\mathcal{F} := F(z)^{\sigma^{an-1}} \cdot F(z)^{\sigma^{an-2}} \cdots F(z)^{\sigma} \cdot F(z)$$

as explained by Kedlaya in [13] and find $Z(T)$ as the polynomial over \mathbb{Z} , congruent to $\det(I - \mathcal{F}T)$ modulo 2^{N_f} , with coefficients between -2^{N_f-1} and 2^{N_f-1} . Output now

$$\frac{Z(T)}{(1-T)(1-2^{an}T)}.$$

PROPOSITION 20. *The above algorithm returns the correct result.*

Proof. The Lefschetz fixed point formula on the Monsky-Washnitzer cohomology gives as explained at the end of Section 3 in [7] that $Z(T)$ does equal $\det(I - \mathcal{F}T)$ if \mathcal{F} would be the exact matrix of the map F_2^n . The theory from Sections 2 and 3 above implies that if every step was done with exact precision, we would indeed find the required matrix \mathcal{F} . As we cannot work with this infinite precision, we need to show that the chosen accuracy is high enough. From the Weil conjectures it follows, see [7, Section 4.1], that $\mathcal{F} \bmod 2^{N_f}$ is sufficient to recover the zeta function as explained in the last part of Step 6. Proposition 11 and Note 12 imply that M and N_Γ are large enough, viz. working modulo Γ^{N_Γ} suffices to compute $r(\Gamma)^M R(\Gamma) F(\Gamma) B(\Gamma)^{-1}$ modulo 2^N . The crucial difficulty is to control the loss of precision introduced by working with non integral elements of \mathbb{Q}_q . It is clear that computing r, B, R and D gives no significant loss in precision. For computing K we can bound the introduced error as in Theorem 13, which gives that the loss in precision is at most N_2 . In Step 5 precision can only be lost during the multiplication with $B(z)^{-1}$, which explains the term $\beta' = (2g-1)(3 + \lfloor \log_2(5g+1) \rfloor)$ in N , $-\beta'$ being a lower bound for the valuation of $B(\Gamma)^{-1}$ as proven at the end of Section 3.3.

We should also take notice of possible loss in accuracy in the computation of \mathcal{F} as a product, which requires an extra $an\phi$ of accuracy. But as pointed out in Note 12, in practice \mathcal{F} turns out to have about the same valuation as $F(\gamma)$, hence this increment of N can in practice be chosen lower. Another problem appears in the computation of the characteristic polynomial of \mathcal{F} . One naive way of doing this would be to compute the trace of \mathcal{F}^i for $i = 1, \dots, 2g$ and to use Newton's formula

$$\det(I - \mathcal{F}T) = \exp \left(- \sum_{k=1}^{\infty} \text{Tr}(\mathcal{F}^k) \frac{T^k}{k} \right),$$

which would require an extra precision of $2g + 2g \log_2(2g)$ from the exponential and the denominators k , and extra precision $2gan\phi$ for the trace of \mathcal{F}^{2g} , where we have to note that the Weil conjectures imply that $\text{Tr}(\mathcal{F}^k)$ is 2-adic integral for all k . A better way however is explained in [2, Section 7.3, Step IX]. Here we first make \mathcal{F} integral by multiplying it with some power of 2, and then use a slightly altered version of reduction to the Hessenberg form of a matrix, suitable for working in \mathbb{Z}_q^n . The loss in precision is then $2gan\phi$. We can conclude that the values of N and N_2 are sufficient. \square

5. Complexity analysis

5.1. 2-Adic arithmetic

As central source for this section we use Chapter 12 in [4] by Vercauteren, and we always assume asymptotically fast arithmetic, meaning that all basic arithmetic operations can be done in quasi-linear time, see [1]. We suppose here that we are working modulo

2^N , hence representing an element of \mathbb{Q}_2 takes $O(N)$ bits (if minus its valuation is not larger than $O(N)$, which will always be satisfied) and computing with it takes $\tilde{O}(N)$ bit operations. Recall that $q = 2^a$. Let $\mathbb{F}_q \cong \mathbb{F}_2[x]/\tilde{\chi}(x)$, then we define $\mathbb{Q}_q \cong \mathbb{Q}_2[x]/\chi(x)$ where χ is the Teichmüller modulus that projects to $\tilde{\chi}$. A Teichmüller modulus $\chi(x)$ is the (monic) minimal polynomial of some Teichmüller lift, or equivalently $\chi(x)|x^q - x$. In Section 12.1.2 of [4] an algorithm of Harley is given that computes χ in time $\tilde{O}(aN)$. Basic arithmetic operations and the 2nd power Frobenius automorphism σ need the same amount of time.

If $\tilde{\psi}(z)$ is the minimal polynomial of $\tilde{\gamma}$ over \mathbb{F}_q , we can compute the Teichmüller modulus $\psi(z)$, being the minimal polynomial of the Teichmüller lift of $\tilde{\gamma}$ over \mathbb{Q}_q , as follows. First determine $\varphi(y)$ such that $\mathbb{Q}_{q^n} \cong \mathbb{Q}_2[y]/\varphi(y)$, $\varphi(y)|y^{2^{an}} - y$ and $\tilde{\varphi}(\tilde{\gamma}) = 0$ as above, in time $\tilde{O}(anN)$. Second, as $\varphi(z) = 0$, we have that $\psi|\varphi$, or $\varphi = \psi \cdot \psi'$ for a suitable ψ' . Now $\tilde{\psi}$ and $\tilde{\varphi}$ are known, hence $\tilde{\psi}'$ can be recovered easily, and using Hensel lifting as in [23] gives ψ in time $\tilde{O}(anN)$. Again this is also the time required for basic arithmetic operations in \mathbb{Q}_{q^n} and the action of σ .

Computing σ^k of an element of \mathbb{Q}_{q^n} can be done trivially by applying k times σ , resulting in a complexity of $\tilde{O}(kanN)$. However, further on it will be advantageous to be able to compute the action of σ^k on the Teichmüller lift z in a faster way. We can compute $\tilde{\gamma}^{2^k}$ in time $\tilde{O}(kan)$ by repeated squaring, and using the generalised Newton lifting of [4] on the equation $X^2 - X^\sigma = 0$ we find the Teichmüller lift of $\tilde{\gamma}^{2^k}$, which equals $\sigma^k(z)$, in time $\tilde{O}(anN)$.

5.2. Analysis of the algorithm and proof of Theorem 1

We use the 2-adic arithmetic always as in the previous paragraph. Let ω be an exponent for matrix multiplication, which means that multiplying two $k \times k$ matrices over some ring R takes $O(k^\omega)$ operations in R . We can take $\omega = 2.376$, see [5]. It is easy to check the following bounds:

$$\begin{aligned} \varphi &= O(\log g) = \tilde{O}(1), \\ N_f, N, N_2 &= \tilde{O}(ang), \\ N_\Gamma &= \tilde{O}(g\kappa N\tilde{D}) = \tilde{O}(g^2 a\kappa n\tilde{D}). \end{aligned}$$

Computing the lifts of \tilde{H} and $\tilde{Q}_{\tilde{f}}$ costs essentially nothing, and the computation of the resultant $r(\Gamma)$ (and $R(\Gamma)$ as resultant later on) can be achieved in time $\tilde{O}(g^{1+\omega} aNg\kappa) = \tilde{O}(g^{3+\omega} a^2\kappa n)$, see for example [22], where we use the fact that we are working with polynomials in Γ of degree at most $O(g\kappa)$. To determine B and D we have to use formula (2) at most $O(g)$ times and each step requires time $\tilde{O}(aN \cdot g\kappa \cdot g)$, where we use that $O(aN)$ is the bit size of an element of \mathbb{Q}_q , the degree in Γ of the polynomials is $O(g\kappa)$ and their degree in X is $O(g)$. Together this gives $\tilde{O}(g^4 a^2 n\kappa)$.

Next we have the recursive formula for finding K . Each of the N_Γ steps consists of $O(g\kappa)$ multiplications of matrices whose entries have size $O(aN)$, resulting in $O(g\kappa g^\omega aNN_\Gamma) = \tilde{O}(g^{4+\omega} a^3 \kappa^2 n^2 \tilde{D})$. The size of K is $O(g^2 aNN_\Gamma) = \tilde{O}(g^5 a^3 \kappa n^2 \tilde{D})$, which will be the overall memory requirements of the algorithm. Note that we can ignore the operations for finding B^σ and the like.

For Step 3 of our algorithm we have to repeat part of the complexity analysis of [7]²,

²In that paper the memory requirements are actually $\log g$ bigger than written there, because the computation of

where we can confine ourselves to the ‘worst case’ mentioned there rather than to look at the ‘average case’. Having only to compute the matrix of the 2nd power Frobenius $F(0)$, Step 4 in the algorithm of [7] is the most time consuming step, taking time $\tilde{O}(g^3 a N^2) = \tilde{O}(g^5 a^3 n^2)$. The memory requirements are $O(g^4 a^3 n^2)$.

The minimal polynomial $\tilde{\Psi}$ in Step 5 can be computed in time $O((an)^2)$, see [19], and finding ψ out of $\tilde{\Psi}$ takes $\tilde{O}(anN)$ bit operations.

Let $f(\Gamma)$ be an entry of $r(\Gamma)^{\chi_1} R(\Gamma) F(\Gamma) B(\Gamma)^{-1}$, then we have to find $f(z)$, being a substitution $\Gamma \leftarrow z$ that can be done very fast using our Teichmüller modulus. Indeed, we just have to reduce $f(z)$ modulo $\psi(z)$, which takes for the whole of the matrix $\tilde{O}(g^2 a N N_\Gamma) = \tilde{O}(g^5 a^3 \kappa n^2 \tilde{D})$ bit operations. Division by $r(z)^{\chi_1} R(z)$ and multiplication by $B(z)$ again can be ignored. We remark that until now, where we have found the matrix of the small Frobenius, our algorithm has essentially a quadratic dependency on n .

For the last step Kedlaya’s method consists of the following iteration: $M_0 := F(z)$ and $M_{i+1} = M_i^{\sigma_i}$. This requires $\log n$ times a matrix multiplication over \mathbb{Q}_q^n , which needs time $\tilde{O}(g^\omega a n N)$, and in addition the computation of σ^k on $4g^2$ elements requires $\tilde{O}(g^2 \cdot k \cdot a n N) = \tilde{O}(g^2 a^2 n^2 N)$ bit operations.

Combining all these facts gives up to Step 5 a complexity of $\tilde{O}(g^{4+\omega} a^3 \kappa^2 n^2 \tilde{D})$ bit operations and $\tilde{O}(g^5 a^3 \kappa n^2 \tilde{D})$ bits of memory. However, as explained in Section 6.2 below, we can remove one factor g from these memory requirements. Now as ‘on average’ $\tilde{D} = O(1)$ — worst case being $\tilde{D} = O(g)$ — this gives the first term in the time complexity and the memory requirements of Theorem 1. Step 6 gives the second part of the time estimate.

6. Improvements

6.1. Subcubic counting.

The most time consuming step in the above algorithm is in fact the determination of $F(z)^{\sigma^k}$ for k of the order $O(an)$, taking time $\tilde{O}(g^3 a^3 n^3)$. It is however possible to do this with a faster method. Let $\alpha(z) \in \frac{\mathbb{Q}_q[z]}{\psi(z)}$, then the equality $\alpha(z)^{\sigma^k} = \alpha^{\sigma^{k \bmod a}}(z^{\sigma^k})$ shows that we only have to compute $4g^2 \log n$ times $\alpha^{\sigma^\ell}(z^{\sigma^k})$ with $\ell = O(a)$ and $k = O(an)$, where α is a polynomial modulo 2^N over \mathbb{Q}_q of degree at most $n - 1$. The computation of α^{σ^ℓ} takes at most time $\tilde{O}(a N \ell n) = \tilde{O}(g a^3 n^2)$. On the other hand we have the *modular composition of polynomials* $\alpha^{\sigma^\ell}(z^{\sigma^k}) \bmod \psi(z)$. As explained at the end of Section 5.1, the computation of z^{σ^k} takes only $\tilde{O}(g a^2 n^2)$ time. Following Sections 6.1 and 6.2 of [12], this modular composition can be achieved in time $\tilde{O}(g a^2 n^{2.667})$, at the cost of an increase in memory use, namely $O(g a^2 n^{2.5})$. Doing this for all $4g^2$ entries gives Theorem 2 from the introduction.

6.2. Using less memory

An easy adaptation of the algorithm presented in Section 4 decreases the memory requirements with a factor g , without increasing the time complexity. The idea is as follows: instead of computing the matrix $K(\Gamma) \bmod 2^{N_2}, \Gamma^{N_\Gamma}$ at once and reducing it modulo $\psi(\Gamma)$ afterwards, we compute $K(\Gamma)$ in parts of length N_Γ/g . After each of the g steps we reduce the result modulo $\psi(\Gamma)$. More precisely, first we compute $K_0, K_1, \dots, K_{N_\Gamma/g}$ and

the characteristic polynomial of the big Frobenius needs to take care of the emerging denominators. Although this factor $\log g$ is removed in the erratum [6], this is irrelevant for us, as we are interested in the 2nd power Frobenius, whereas the problem only appears further on in the algorithm of [7].

$\tilde{K}_1 := \sum_{i=0}^{N_\Gamma/g} K_i \Gamma^i \pmod{\psi(\Gamma)}$. We only need the last $O(g\kappa)$ matrices K_i in order to continue the computation. Next we forget all K_i except these $O(g\kappa)$ last ones, and continue with $K_{N_\Gamma/g+1}, \dots, K_{2N_\Gamma/g}$ and $\tilde{K}_2 := \sum_{i=N_\Gamma/g+1}^{2N_\Gamma/g} K_i \Gamma^i \pmod{\psi(\Gamma)}$. This can be done until the end, and the result is then

$$K(z) \equiv (K(\Gamma) \pmod{\psi(\Gamma)}) \equiv \sum_{i=1}^g \tilde{K}_i \pmod{2^{N_2}}.$$

Finally we multiply $K(z)$ with $B(z)/(r(z)^M R(z))$ and find $F(z)$. It is easy to verify that the global time complexity does not increase, whereas the memory requirements drop with a factor g .

6.3. Lots of curves.

Using fast multipoint evaluation and fast matrix multiplication it is possible to compute n zeta functions within one family in time $\tilde{O}(n^{3.376})$ and memory $O(n^3)$. We do not go into all the details, but the main steps needed for this estimate are the following. Suppose $a = 1$, and we only look at the dependency on n . As before we compute $r(\Gamma)^{\chi_1} R(\Gamma) F(\Gamma) B(\Gamma)^{-1}$ in time $\tilde{O}(n^2)$, and some Teichmüller modulus $\psi(z)$. Let $\tilde{\gamma}_1, \dots, \tilde{\gamma}_n$ be the parameters for which we want to calculate the zeta function. Computing all the Teichmüller lifts $\gamma_1, \dots, \gamma_n$ takes $\tilde{O}(n^3)$ time. Next there are two main points. First we can use fast multipoint evaluation to compute all the matrices $F(\gamma_i)$ at once in time $\tilde{O}(n^3)$ and space $O(n^3)$, and second we can compute for $k = O(n)$ and a set $\{\alpha_i\}_{i=1}^n \subset \mathbb{Q}_{2^n}$ all the values $\sigma^k(\alpha_i)$ in time $\tilde{O}(n^{3.376})$ and space $O(n^3)$ using fast matrix multiplication. In going from $F(\gamma_i)$ to $\mathcal{F}(\gamma_i)$ for all i this is the only step requiring more time than $\tilde{O}(n^3)$ and hence the result follows.

We explain first how to compute all the matrices $\mathcal{F}(\gamma_i)$ together in time $\tilde{O}(n^3)$. Let the ring R be equal to \mathbb{Z}_{2^n} considered modulo 2^N , then Corollary 10.8 in [23] says the following: We can evaluate any polynomial in $R[\Gamma]$ of degree less than n at n elements of R using $\tilde{O}(n^2)$ operations in R . For our situation we need degree $O(n)$ instead of ‘less than n ’ — but this is an immediate consequence of the corollary — and memory requirements equivalent to representing at most $O(n^2)$ elements of R , which is easily derived from the proof of the corollary. The matrix $2^\varphi F(\Gamma)$ consists of polynomials in $\mathbb{Z}_{2^n}[\Gamma]$ (in fact, in $\mathbb{Z}_2[\Gamma]$) modulo $2^{N+\varphi}$ of degree $O(n)$, and hence we can find all matrices $\mathcal{F}(\gamma_i)$ in time $\tilde{O}(n^3)$ and space $O(n^3)$.

Next we have n elements $\alpha_i(z) \in \mathbb{Q}_{2^n} = \mathbb{Q}_2[z]/\psi(z)$. We fix some power k of σ and compute first $\beta(z) := \sigma^k(z)$ and the powers $\beta_j(z) := \beta(z)^j$ for $j = 0, \dots, n-1$. This can certainly be done in time $\tilde{O}(n^3)$. We write

$$\alpha_i(z) = \sum_{j=0}^{n-1} a_{i,j} z^j \quad \text{and} \quad \beta_j(z) = \sum_{\ell=0}^{n-1} b_{j,\ell} z^\ell.$$

With A the matrix over \mathbb{Q}_2 consisting of the entries $a_{i,j}$ and similar B for the $b_{j,\ell}$, we have to compute

$$\sigma^k(\alpha_i(z)) = \alpha_i(\beta(z)) = \sum_{j=0}^{n-1} \sum_{\ell=0}^{n-1} a_{i,j} b_{j,\ell} z^\ell \quad \text{or} \quad \begin{pmatrix} \sigma^k(\alpha_1(z)) \\ \vdots \\ \sigma^k(\alpha_n(z)) \end{pmatrix} = A \cdot B \cdot \begin{pmatrix} z^0 \\ \vdots \\ z^{n-1} \end{pmatrix}.$$

We can conclude that we only have to compute the product of A and B , which requires $O(n^{2.376})$ operations in \mathbb{Q}_2 , as proven in [5].

Note that this result is also applicable to the situation in [12], hence for hyperelliptic curves in odd characteristic.

6.4. Quadratic counting with GNB.

If we work over fields \mathbb{F}_{q^n} where a Gaussian normal basis (GNB) of type t for some small t exists (see [4, Section 2.3.3.b], and [14] for the existence of such bases), then we can make our algorithm quadratic for some well-chosen parameters. Here is an outline of how this works for $t = 1$ and $a = 1$, which means we have a representation

$$\mathbb{F}_{2^n} \cong \frac{\mathbb{F}_2[x]}{x^n + x^{n-1} + \cdots + x + 1}.$$

The same minimal polynomial $(x^{n+1} - 1)/(x - 1)$ can be used over \mathbb{Q}_2 to represent \mathbb{Q}_{2^n} , and it is clear that it is a Teichmüller modulus. Note that $x^{n+1} = 1$, which makes computing a lot easier. Suppose now that our parameter γ equals some power of x , say x^k . We note that this is a very strong condition, for there exist only $n + 1$ such parameters γ . As explained earlier the crucial step is computing $\alpha(\gamma)^{\sigma^\ell}$ for $\ell = O(n)$ and α some polynomial of degree $O(n)$ over \mathbb{Q}_2 modulo $2^{O(n)}$. Now if $\alpha(\Gamma) = \sum_{i=0}^m a_i \Gamma^i$, then we have (using a *redundant representation*, a non-unique form using the generating set $1, x, \dots, x^n$)

$$\alpha(\gamma)^{\sigma^\ell} = \alpha(x^{2^\ell k}) = \sum_{i=0}^m a_i x^{2^\ell k i \bmod n+1},$$

and this last expression is easily evaluated. We can conclude that this GNB allows us to compute the zeta function for certain parameters in time $\tilde{O}(n^2)$. Here too we can draw the same conclusions for the odd characteristic case.

References

1. DANIEL J. BERNSTEIN, ‘Fast multiplication and its applications.’ URL: <http://cr.ypt.to/papers.html#multapps>. To appear in Buhler-Steinhagen’s *Algorithmic number theory*.
2. W. CASTRYCK, J. DENEFF and F. VERCAUTEREN, ‘Computing zeta functions of nondegenerate curves.’ *IMRP Int. Math. Res. Pap.* (2006) Art. ID 72017, 57.
3. ANTOINE CHAMBERT-LOIR, ‘Compter (rapidement) le nombre de solutions d’équations dans les corps finis.’ *Séminaire Bourbaki*, 59e année, Novembre 2006.
4. HENRI COHEN, GERHARD FREY, ROBERTO AVANZI, CHRISTOPHE DOCHE, TANJA LANGE, KIM NGUYEN and FREDERIK VERCAUTEREN (eds), *Handbook of elliptic and hyperelliptic curve cryptography*. Discrete Mathematics and its Applications (Boca Raton) (Chapman & Hall/CRC, Boca Raton, FL, 2006). ISBN 978-1-58488-518-4; 1-58488-518-1.
5. DON COPPERSMITH and SHMUEL WINOGRAD, ‘Matrix multiplication via arithmetic progressions.’ *J. Symbolic Comput.* 9 (1990) 251–280.
6. JAN DENEFF and FREDERIK VERCAUTEREN, ‘Errata for “An extension of Kedlaya’s algorithm to hyperelliptic curves in characteristic 2”, and related papers.’ Available on http://www.wis.kuleuven.be/algebra/denef_papers/ErrataPointCounting.pdf.

7. JAN DENEFF and FREDERIK VERCAUTEREN, ‘An extension of Kedlaya’s algorithm to hyperelliptic curves in characteristic 2.’ *J. Cryptology* 19 (2006) 1–25. Erratum available as [6].
8. NOAM D. ELKIES, ‘Elliptic and modular curves over finite fields and related computational issues.’ ‘Computational perspectives on number theory (Chicago, IL, 1995),’ (Amer. Math. Soc., Providence, RI, 1998), vol. 7 of *AMS/IP Stud. Adv. Math.* pp. 21–76, pp. 21–76.
9. PIERRICK GAUDRY and ROBERT HARLEY, ‘Counting points on hyperelliptic curves over finite fields.’ ‘Algorithmic number theory (Leiden, 2000),’ (Springer, Berlin, 2000), vol. 1838 of *Lecture Notes in Comput. Sci.* pp. 313–332, pp. 313–332.
10. RALF GERKMANN, ‘Relative rigid cohomology and deformation of hypersurfaces.’ To appear in *Intern. Math. Research Papers*.
11. RALF GERKMANN, ‘Relative rigid cohomology and point counting on families of elliptic curves.’ Preprint, available on <http://www.mathematik.uni-mainz.de/~gerkmann/>.
12. HENDRIK HUBRECHTS, ‘Point counting in families of hyperelliptic curves.’ To appear in *Foundations of Computational Mathematics*.
13. KIRAN S. KEDLAYA, ‘Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology.’ *J. Ramanujan Math. Soc.* 16 (2001) 323–338.
14. H. Y. KIM, J. Y. PARK, J. H. CHEON, J. H. PARK, J. H. KIM and S. G. HAHN, ‘Fast elliptic curve point counting using Gaussian normal basis.’ *Algorithmic Number Theory Symposium - ANTS V, Lecture Notes in Computer Science* 2369 (2002) 292–307.
15. ALAN G. B. LAUDER, ‘Deformation theory and the computation of zeta functions.’ *Proc. London Math. Soc.* (3) 88 (2004) 565–602.
16. ALAN G. B. LAUDER, ‘Rigid cohomology and p -adic point counting.’ *J. Théor. Nombres Bordeaux* 17 (2005) 169–180.
17. ALAN G. B. LAUDER, ‘A recursive method for computing zeta functions of varieties.’ *LMS J. Comput. Math.* 9 (2006) 222–269 (electronic).
18. TAKAKAZU SATOH, ‘The canonical lift of an ordinary elliptic curve over a finite field and its point counting.’ *J. Ramanujan Math. Soc.* 15 (2000) 247–270.
19. VICTOR SHOUP, ‘Efficient Computation of Minimal Polynomials in Algebraic Extension of Finite Fields.’ *Proc. 1999 International Symposium on Symbolic and Algebraic Computation*.
20. N. TSUZUKI, ‘Bessel F -isocrystals and an algorithm of computing Kloosterman sums.’ Preprint.
21. FREDERIK VERCAUTEREN, *Computing zeta functions of curves over finite fields* (PhD thesis, KULeuven, Belgium, 2003).
22. GILLES VILLARD, ‘Computation of the inverse and determinant of a matrix.’ *Algorithm Seminar 2001-2002, F. Chyzak (ed.), INRIA* (2003) 29–32.
23. JOACHIM VON ZUR GATHEN and JÜRGEN GERHARD, *Modern computer algebra* (Cambridge University Press, Cambridge, 2003). ISBN 0-521-82646-2.

Hendrik Hubrechts Hendrik.Hubrechts@wis.kuleuven.be

Department of mathematics, Katholieke Universiteit Leuven

Celestijnenlaan 200B - bus 2400

3001 Leuven

Belgium